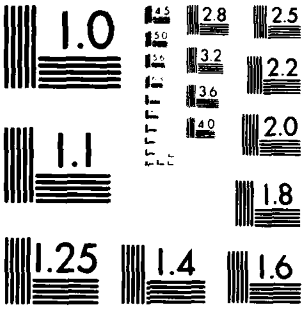
AD-A089 696 SRI INTERNATIONAL MENLO PARK CA F/G 15/3
AN ASSESSMENT OF AVAILABLE SECURITY SYSTEM SIMULATIONS TO SUPPO--ETC(U)
FEB 79 R H MONAHAN, E L DUBOIS DNA001-78-C-0321
UNCLASSIFIED DNA-4886F NL

1 of 2
AD
A089696


1.0
4.5
5.0
5.6
2.8
3.2
3.6
4.0
2.5
2.2
2.0
1.1
1.8
1.25
1.4
1.6

PHOTOGRAPH THIS SHEET

AD A089696

DTIC ACCESSION NUMBER

II

LEVEL

I

INVENTORY

SRI International
Menlo Park, CA
Final Report for Period 30 May '78 - 31 Dec. '78
Dtd. 28 Feb. '1979
DNA 4886F

DOCUMENT IDENTIFICATION

Contract No. DNA001-78-C-0321

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

DISTRIBUTION STATEMENT

| | | |
|---|---|---|
| ACCESSION FOR | | |
| NTIS GRA&I | ☒ | |
| DTIC TAB | □ | |
| UNANNOUNCED | □ | |
| JUSTIFICATION | | |
| | | |
| | | |
| | | |
| BY | | |
| DISTRIBUTION / | | |
| AVAILABILITY CODES | | |
| DIST | AVAIL AND/OR SPECIAL | |
| A | | |

DISTRIBUTION STAMP

DATE ACCESSIONED

80 9 29 070

DATE RECEIVED IN DTIC

PHOTOGRAPH THIS SHEET AND RETURN TO DTIC-DDA-2

FC7D

DNA 4886F

# AN ASSESSMENT OF AVAILABLE SECURITY SYSTEM SIMULATIONS TO SUPPORT THE TNFS$^2$ PROGRAM

SRI International
333 Ravenswood Avenue
Menlo Park, California 94025

28 February 1979

Final Report for Period 30 May 1978—31 December 1978

CONTRACT No. DNA 001-78-C-0321

APPROVED FOR PUBLIC RELEASE;
DISTRIBUTION UNLIMITED.

THIS WORK SPONSORED BY THE DEFENSE NUCLEAR AGENCY
UNDER RDT&E RMSS CODE B390078465 A99QAXFC30901 H2590D.

Prepared for
Director
DEFENSE NUCLEAR AGENCY
Washington, D. C. 20305

Destroy this report when it is no longer needed. Do not return to sender.

PLEASE NOTIFY THE DEFENSE NUCLEAR AGENCY, ATTN: STTI, WASHINGTON, D.C. 20305, IF YOUR ADDRESS IS INCORRECT, IF YOU WISH TO BE DELETED FROM THE DISTRIBUTION LIST, OR IF THE ADDRESSEE IS NO LONGER EMPLOYED BY YOUR ORGANIZATION.

DNA PRINTING PLANT

# REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS
BEFORE COMPLETING FORM

| | | |
|---|---|---|
| 1. REPORT NUMBER<br>DNA 4886F | 2. GOVT ACCESSION NO. | 3. RECIPIENT'S CATALOG NUMBER |

4. TITLE (and Subtitle)
AN ASSESSMENT OF AVAILABLE SECURITY SYSTEM SIMULATIONS TO SUPPORT THE TNFS$^2$ PROGRAM

5. TYPE OF REPORT & PERIOD COVERED
Final Report for Period
30 May 78—31 Dec 78

6. PERFORMING ORG. REPORT NUMBER
SRI Project 7479

7. AUTHOR(s)
Richard H. Monahan
Edmund L. DuBois

8. CONTRACT OR GRANT NUMBER(s)
DNA 001-78-C-0321

9. PERFORMING ORGANIZATION NAME AND ADDRESS
SRI International
333 Ravenswood Avenue
Menlo Park, California 94025

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
Subtask A99QAXFC309-01

11. CONTROLLING OFFICE NAME AND ADDRESS
Director
Defense Nuclear Agency
Washington, D.C. 20305

12. REPORT DATE
28 February 1979

13. NUMBER OF PAGES
136

14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)

15. SECURITY CLASS (of this report)
UNCLASSIFIED

15a. DECLASSIFICATION DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

This work sponsored by the Defense Nuclear Agency under RDT&E RMSS Code B390078465 A99QAXFC30901 H2590D.

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

| | |
|---|---|
| Nuclear Weapons | Performance Measures |
| Security Systems | Testing |
| Simulation Models | |

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This research effort involved an analysis of existing computer simulations to determine the availability of suitable simulations that could be used to evaluate the effectiveness of security systems and concepts in support of Theater Nuclear Force (TNF) weapons during peacetime. The report, in addition to presenting analyses of existing simulations, summarizes security system requirements, identifies threat elements, discusses

20. ABSTRACT (Continued)

possible performance measures, and indicates an interface of simulations with a test program. Although several simulations are directly applicable to the purpose of supporting the TNFS$^2$ Program, a significant amount of simulation development will still be required.

# EXECUTIVE SUMMARY

## Purpose and Scope

The purpose of this research effort is to assist the Defense Nuclear Agency (DNA) in their efforts to determine the simulation tools requirements in support of the Theater Nuclear Force Security and Survivability ($TNFS^2$) Program. This particular research effort involved an analysis of existing computer simulations to determine the availability of suitable simulations that could be used by DNA to evaluate the effectiveness of security systems and concepts in support of Theater Nuclear Force (TNF) weapons. The scope of this effort was restricted to peacetime security operations in the NATO theater of operations, although some consideration was given to the transition period from peacetime to open hostilities.

## Background

A critical requirement imposed on NATO forces is the maintenance of the security of TNF weapons within NATO at various stages leading up to, and including, open hostilities between NATO and Warsaw Pact forces. During peacetime, most weapons are stored at sites that are presumably known to various adversary groups (Warsaw Pact forces, enemy agents, terrorist groups, and individual fanatics), and hence are prime targets for sabotage, pilfering, and disruptive rioting. Transport of TNF weapons during peacetime is also likely through both the initial stockpiling of weapons and the transfer of weapons from one site to another for logistical or political reasons. Although these movements are generally conducted in secrecy, intelligent observers can detect abnormal activity that may indicate preparation for movement. Thus, the security of these weapons while in transport is particularly sensitive. In crises that could lead to open hostilities, movement of TNF weapons to dispersed field storage locations is likely, and this imposes an added burden on the NATO forces. During these periods, however, the troops will be in a high level of alert, and stringent security measures will be in effect. At the onset of open hostilities, survivability of TNF weapons will become the primary objective, although security will still have to be maintained.

DNA is responsible for evaluating requirements to ensure that adequate procedures, material, and personnel are provided to maintain the security of TNF weapons in NATO Europe at the highest level possible. Therefore, it is necessary to evaluate the effectiveness of alternative procedures, equipment, and personnel allocations as they relate to the maintenance and enhancement of the security of TNF weapons. One means of performing these evaluations is through simulation. Simulation analysis is an extremely useful and economical tool for evaluating a broad range of concepts and alternative systems under a variety of postulated environments. Thus, it is highly beneficial to DNA to determine the availability and usefulness of simulations that could be used in their security systems evaluations.

## Method of Approach

The analysis was conducted in essentially four stages. The first stage involved a review of existing documentation and discussions with knowledgeable personnel to identify security system requirements in the protection of TNF weapons, to establish the threat spectrum of concern, and to establish a systematic representation of the kinds of events to which TNF weapons are subjected from arrival in the theater to their ultimate disposition.

The second stage of the analysis involved the identification of performance measures that would provide a quantitative basis for evaluating the effectiveness of existing or postulated security systems and concepts in maintaining the security of TNF weapons.

The third stage was directed to establishing how simulations could interface with testing to enhance the overall utility of the $TNFS^2$ Program.

The fourth stage of the analysis was concerned with the identification of simulations that could provide direct support to the $TNFS^2$ Program. The effort involved the conduct of a literature search to identify existing simulations that might be applicable to the support of the $TNFS^2$ Program and the subsequent detailed analysis of the selected simulations to determine their degree of applicability.

The results of the analysis indicated the need for additional simulation development to support the $TNFS^2$ Program. A seven-task program directed to the future development of simulation tools to support the $TNFS^2$ Program is recommended.

## Security Requirements

The policy guidelines established by the Department of Defense for the security of nuclear weapons call for security in depth; for comprehensive physical and personnel security systems; for the use of every means available to ensure security (including deadly force if necessary); for compensatory measures to maintain standards whenever circumstances mandate waiver or exception to established criteria; and inspections, surveys, and certifications to ensure compliance. The policy does explicitly correlate nuclear weapon protection requirements to the threat existing at any time: An increased threat dictates an increase in security measures. In this respect, the policy establishes security requirements--over and above mandatory minimum requirements--in proportion to the threat.

In response to the broad policies and requirements established by the Office of the Secretary of Defense, standards, criteria, procedures, and equipment to ensure nuclear weapon security are specified by the Military Departments and field commands in great detail. The elements that comprise the current security program and the general nature of the standards, criteria, and methods provide a basis for assessing how simulations may be applied to evaluate system improvement. It is to be expected that the philosophy and principles--and much of the detail--of the security program as currently promulgated will remain valid despite future changes in theater nuclear posture.

The DoD requirements to use every means available to safeguard weapons are explicit. The fact that deadly force is to be used where necessary, including situations where hostages have been taken, is indicative of the seriousness attached to the security mission. The requirement for security in depth involves multiple, redundant, and sequential safeguards of all kinds. This extends to barrier systems, warning systems, communication systems, personnel behavioral safeguards, security forces, and other aspects. The categories of restricted, limited, and exclusion areas prescribed around nuclear weapons at all times and the graded access and human reliability controls applied to these controlled areas reflects the principle of sequential safeguards in depth. Strict inspections, security surveys, and certification of facility, equipment, transportation adequacy, and personnel proficiency and reliability ensure that criteria are met.

Major reliance is placed on physical security means, but in no case is sole reliance placed on physical security without human backup. There are careful controls under the Personnel Reliability Program to guard against aberrant behavior of personnel who may have access to, or knowledge of, nuclear weapons. The two-man concept to protect against incorrect or unauthorized procedures is rigidly applied as one means to guard against both inadvertent and deliberate acts that could degrade weapon performance. An important aspect of security requirements is the importance attached to correct interpretation of the intent and temper of any suspected or attempted breach of security. This is necessary to guard against using excessive force in response to innocent trespassing or encroachment, but, equally important, it is essential for timely, adequate response to fast-moving events in an intended forceful breach.

Movement of nuclear weapons is to be kept to the minimum consistent with operational requirements. Nevertheless, short-distance ground movements and longer-distance air movements are a frequent occurrence. Routine and emergency procedures, guard forces, movement planning, vehicle inspection and certification, communications, and other requirements are spelled out in detail. Presently, the preferred mode of transportation of nuclear weapons is by air. However, the threat of man-portable ground-to-air precision weapons in the hands of terrorist organizations could conceivably force a shift away from air movement in favor of ground movement for both short and long hauls. Moreover, in situations where large numbers of nuclear weapons are dispersed to field storage, ground movement may be the normal means of transportation if helicopter resources prove to be inadequate to handle the volume of traffic.

## Threat

Under conditions of peace and crisis, threats to the security of nuclear weapons in Europe and other overseas theaters include both inadvertent and deliberate actions, and can arise from the actions of persons who are ostensibly friendly and persons who are openly hostile. Although there does not appear to be evidence of a significant increase in subversive activities against military elements by individuals acting alone, there is abundant, well-documented evidence of an increase in overt and covert actions by organized groups against institutions of society and government, including military elements. In particular, the marked upsurge over the past two decades in organized international and transnational terrorism constitutes a very serious threat to military establishments.

There does not seem to be a basis for expecting that this threat will abate in the near future. It may well increase, especially from groups that depend on their own resources rather than on support by sovereign nations. In addition, the Soviet Union clearly has the capabilities to initiate or sponsor forceful actions against nuclear weapons and forces as priority war targets. The use of special forces or airborne forces by the Soviet Union (or other East European countries) in clandestine operations is a capability that could be seriously detrimental.

The extreme political sensitivity attached to nuclear weapon security tends to lower the threshold of threat actions that constitute serious security incidents. Thus a forceful demonstration of capability to penetrate a nuclear security system, even if not carried to the point of actual penetration, can be a useful objective for a group seeking a political aim and a serious erosion of public confidence in security effectiveness. Likewise, an action that physically endangers a nuclear weapon--such as launching a missile against an aircraft or a truck carrying nuclear weapons--might lead to serious political perturbations and gain a terrorist organization needed publicity on a worldwide scale, even if no harm to the weapons results. This potential for leveraging what would be minor threat incidents with most weapons into major threat incidents when nuclear weapons are involved magnifies the problem facing the nuclear weapon security system.

By the same token, more serious actions such as damage, detonation, or capture of a weapon or weapon component can become prime objectives for terrorist political purposes out of all proportion to the imminent danger to U.S. national security. If a single action of this kind is carried out with even limited success, there might well be such severe political reactions by the United States or its allies that theater nuclear force readiness could be reduced by the resulting inhibiting constraints. Security system effectiveness must be measured by its ability to guard against only partially successful breaches and demonstrations of security weakness as well as more destructive actions.

Whether fanatic or terrorist or military force, the attacker will depend on surprise, diversion, deception, confusion, ambush, speed, and shock effect. Enough can be learned by threat organizations about nuclear security activities, patterns, storage locations, guard force size, weapons, and barriers to provide a basis for attack planning and timing. Modern weapons such as man-portable homing missiles, smoke agents, chemical agents, and laser guided weapons can be acquired and used.

## Performance Measures

The overall objective of the total security system for theater nuclear weapons is to maintain the security of the weapons. This includes not only the protection of theater nuclear weapons from damage, destruction, or diversion, but also the avoidance of any incidents, whether intended or not, whose direct or indirect effects could have noticeable political repercussions or could lead to hostile actions. Thus, any measure of the overall performance capabilities of a security system should be directly related to the probability of occurrence of these events over some broad time span. Due to the nature of the TNFS$^2$ Program, which is directed toward improvements in selected aspects of the present security system, a broad performance measure that covers all security system functions would most likely be relatively insensitive to many of the individual improvement options. A more fruitful approach is to adopt performance measures that address the different functional aspects of a security system.

Six basic functions of a security system have been identified. These are dissuasion, detection, assessment, communication, delay, and neutralization. Dissuasion refers to the deterrent and secrecy aspects of a security system that reduce the likelihood of an adversary attempting to breach the system. Detection addresses the function of determining that a possible breach may be underway. The assessment function involves the analysis of detection information to determine if, indeed, responsive action is required and, if it is, to determine the proper response to be taken. The communication function is concerned with informing the security forces (local or back-up) that an adversary action is taking place or is imminent. The delay function encompasses all activities that slow or stop an adversary in the performance of his mission. The neutralization function refers to the actions taken by the security system in countering an adversary action.

A set of performance measures were identified that would be useful in evaluating modifications to security systems and concepts or in comparing alternative security systems. The table on the next page lists the selected performance measures for each security system function.

## Simulation/Testing Interface

Computer simulations, if properly designed and applied, can be extremely valuable tools to be used in support of test programs directed to evaluating the effectiveness of TNF security systems under operational conditions. The constraints of both time and cost impose severe

PERFORMANCE MEASURES

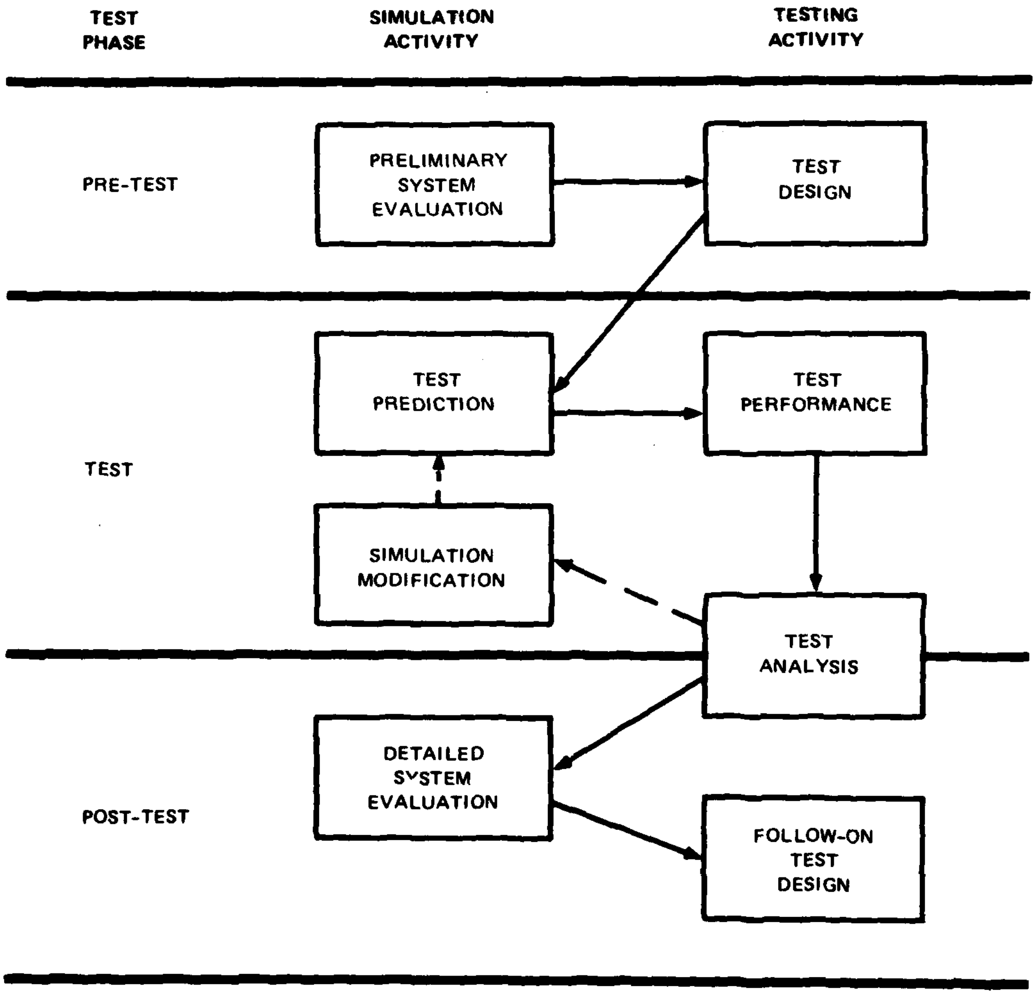
| Security System Function | Performance Measures |
|---|---|
| Dissuasion | Expectation by an adversary of losses to be incurred<br>Minimum adversary resource value required to assure a specified probability of success<br>Probability that an adversary has timely knowledge of a weapon storage location (storage case)<br>Probability that an adversary has timely knowledge of movement events (movement case) |
| Detection | Cumulative probability of initial detection as a function of penetration distance remaining (storage case)<br>Cumulative probability of detection as a function of time prior to an imminent confrontation (movement case)<br>False alarm rate |
| Assessment | Assessment delay time<br>Probability of making a correct assessment<br>False alert rate<br>Nuisance alarm rate |
| Communication | Communication delay time<br>Probability that the minimum required information is received |
| Delay | Penetration delay times |
| Neutralization | Cumulative probability of adversary penetration as function of depth of penetration<br>Probability that a weapon is destroyed<br>Probability that a weapon is damaged<br>Probability that a weapon is stolen<br>Probability that classified information is obtained<br>Probability of using excess force against inadvertent or peaceful intruders<br>Probability that an aircraft transporting the weapons survives to its destination<br>Probability that an aircraft transporting the weapons makes a successful forced landing |

limitations on the amount and scope of testing that can be conducted. Furthermore, certain facets of security system operations are untestable due to safety considerations. With proper planning, simulations can expand the scope and depth of the evaluation process in addition to providing valuable insights for use in test planning. Testing, on the other hand, can enhance the credibility of simulation outputs by providing near-real-life results that can be used for simulation validation and/or calibration. Thus, simulation and testing can interact synergistically with one another to provide for a broad-based, efficient evaluation program.

The interface between simulation and testing can take many forms, depending on the level of testing, the simulation credibility and complexity, the attitudes of the test planners and analysts toward simulations, plus many other factors. The figure on the next page illustrates one representative interface for a system (equipment, personnel, and procedures) that is either in existence or at least adequately designed to be configured for system testing.

There are several important characteristics that simulations should possess in order to be of useful assistance in the conduct of a testing program. These are as follows:

- Completeness--Simulations must adequately cover the broad range of possible confrontation situations and address each of the measurable security system functions.
- Dual complexity--It is desirable to have available simulations of two different levels of complexity: a set of relatively aggregated simulations, and a set of detailed simulations.
- Modularity--The demand for change and improvement mandates that distinct functions be isolated, if possible, in separate programming modules.
- Test compatibility--Simulation inputs and outputs must be compatible with test parameters.
- Machine dependence--Simulations in support of a large test program should be programmed in a universal language and not be burdened with any machine-dependent operations.
- Usability--Simulations must be capable of near-real-time support during the test phase of a test program.



SIMULATION/TESTING INTERFACE

## Availability of Simulation Tools

A literature search was conducted to identify those simulations that might be applicable for use in support of the TNFS$^2$ Program. An initial screening of over 1,100 report abstracts and subsequent activity resulted in identifying 129 reports that appeared directly relevant. A cursory review of these reports led to the identification of 41 simulations as possible candidates. These were subjected to a more detailed analysis, and the following ten simulations that sufficiently address the security system evaluation problem were identified:

- Pathfinding Codes (Sandia Laboratories)--The Pathfinding Codes are a set of computer codes used to establish optimum paths for adversaries to follow in covert sabotage, control, or theft attempts against fixed nuclear sites.

- EASI (Sandia Laboratories)--The Estimate of Adversary Sequence Interruption (EASI) simulation is an aggregated, analytic simulation that provides an estimate of the security system's capability to interrupt an adversary's attempt to sabotage or steal nuclear material at a fixed nuclear site. "Interruption" refers to a response force arriving at the adversary's terminal point [location of nuclear material (weapons) for sabotage and site exit point for theft] prior to the adversary's arrival there.

- FESEM (Sandia Laboratories)--The Forcible Entry Safeguards Effectiveness Model (FESEM) is a combined time-stepped, event-sequenced Monte Carlo simulation designed to evaluate the effectiveness of a security system against covert attempts by an adversary force to sabotage or steal nuclear material (weapons) from a fixed nuclear site.

- VISA (Science Applications, Inc.)--Vulnerability of Integrated Safeguards Analysis (VISA) is an evaluation method that can be used to evaluate the effectiveness of fixed-site security systems against hostile encounters, both overt and covert.

- Schaffer's Ambush Model (Naval Postgraduate School)--The Schaffer Ambush Model is a mixed Lanchester linear/square-law attrition simulation that is representative of the many Lanchester-type simulations that could be used to evaluate the outcomes of transport vehicle ambushes.

- SOURCE (Sandia Laboratories)--The SOURCE code is a time-stepped Monte Carlo simulation to evaluate the initial stages of an ambush of a nuclear material transport convoy. This simulation considers the effects of the ambusher's fire, but does not simulate return fire from the convoy personnel.

- SABRES (Sandia Laboratories)--The SABRES code is a time-stepped Monte Carlo simulation to evaluate the outcomes of engagements between attackers and defenders after a transport vehicle has been stopped. This simulation, developed to analyze the combat activities following the initial stages of an ambush, is used in conjunction with the SOURCE code to analyze the complete ambush confrontation.
- TSEM (The BDM Corporation)--The Transportation Safeguards Effectiveness Model (TSEM) is a simulation designed to evaluate the outcomes of ambush attempts by an adversary force against a defended ground transport convoy carrying critical cargo such as special nuclear material.
- PENAIR (Naval Postgraduate School)--The PENAIR simulation is a time-stepped stochastic simulation developed to evaluate the effectiveness of alternative defensive tactics for an unarmed aircraft while overflying hostile terrain.
- Armed Escort Model (Electronics Associates, Inc.)--The Armed Escort Model is a time-stepped, Monte Carlo simulation designed to evaluate the effectiveness of an armed escort helicopter in protecting a formation of troop carrying helicopters against a single ground weapon, where the ground weapon is located in near proximity to the lift aircraft's landing zone.

These simulations were analyzed in greater detail, using the six simulation characteristics (completeness, dual complexity, modularity, test compatibility, machine independence, and usability) as guidelines.

Based on the results of this research effort, there are a number of conclusions that can be drawn with respect to the availability of simulation tools that would be directly applicable to the TNFS$^2$ Program. Some of these hold in general, while others are directed specifically to Fixed Site Simulations, Ground Transport Simulations, or Air Transport Simulations. These conclusions are as follows:

- General
  - Simulations developed for purposes other than security system evaluation are not, in general, easily adaptable for the purpose of security system evaluation.
  - Simulations developed for the purpose of security system evaluation do provide an adequate base of departure for the development of TNF security system evaluation simulations.

- The simulations reviewed are directed to a single-weapon status state (fixed site, ground transport, or air transport) and thus do not address the transitional operations involved in going from one state to another.
- For the purposes of the TNFS$^2$ Program, a significant amount of simulation development activity will be required, especially if the Dual-Complexity characteristic is desired.
- Sandia Laboratories has amassed a broad security system data base that will be of use for the TNFS$^2$ Program. Users, though, should be knowledgeable as to the existing data voids.

• <u>Fixed Site Simulations</u>

- The Forcible Entry Safeguards Effectiveness Model (FESEM) developed by Sandia Laboratories is one simulation that is directly applicable to TNF security system evaluation. Some modification and expansion will be required. The program uses the FORTRAN-based GASP-IV simulation language, which may pose some minor problems in transferral to an alternate computer system.
- The VISA methodology developed by Science Applications, Inc. provides an alternative approach to FESEM. This would also require some modification for TNF security system evaluation purposes. A network simulation program utilizes the FORTRAN-based Q-GERT queueing network simulation language, which could pose problems.
- Desirable features of both FESEM and VISA could be combined to provide an initial baseline simulation from which to build for TNF security system evaluation purposes.
- Sandia Laboratories' aggregated model EASI (Estimate of Adversary Sequence Interruption) is too aggregated even for use as an aggregated simulation in support of the TNFS$^2$ Program. Furthermore, it does not consider the neutralization function.
- None of the fixed-site simulations reviewed address the problem of false detections and false alarms.
- None of the detailed or aggregated infantry combat simulations surveyed appear to be directly useful for fixed-site security system evaluations.

• <u>Ground Transport Simulations</u>

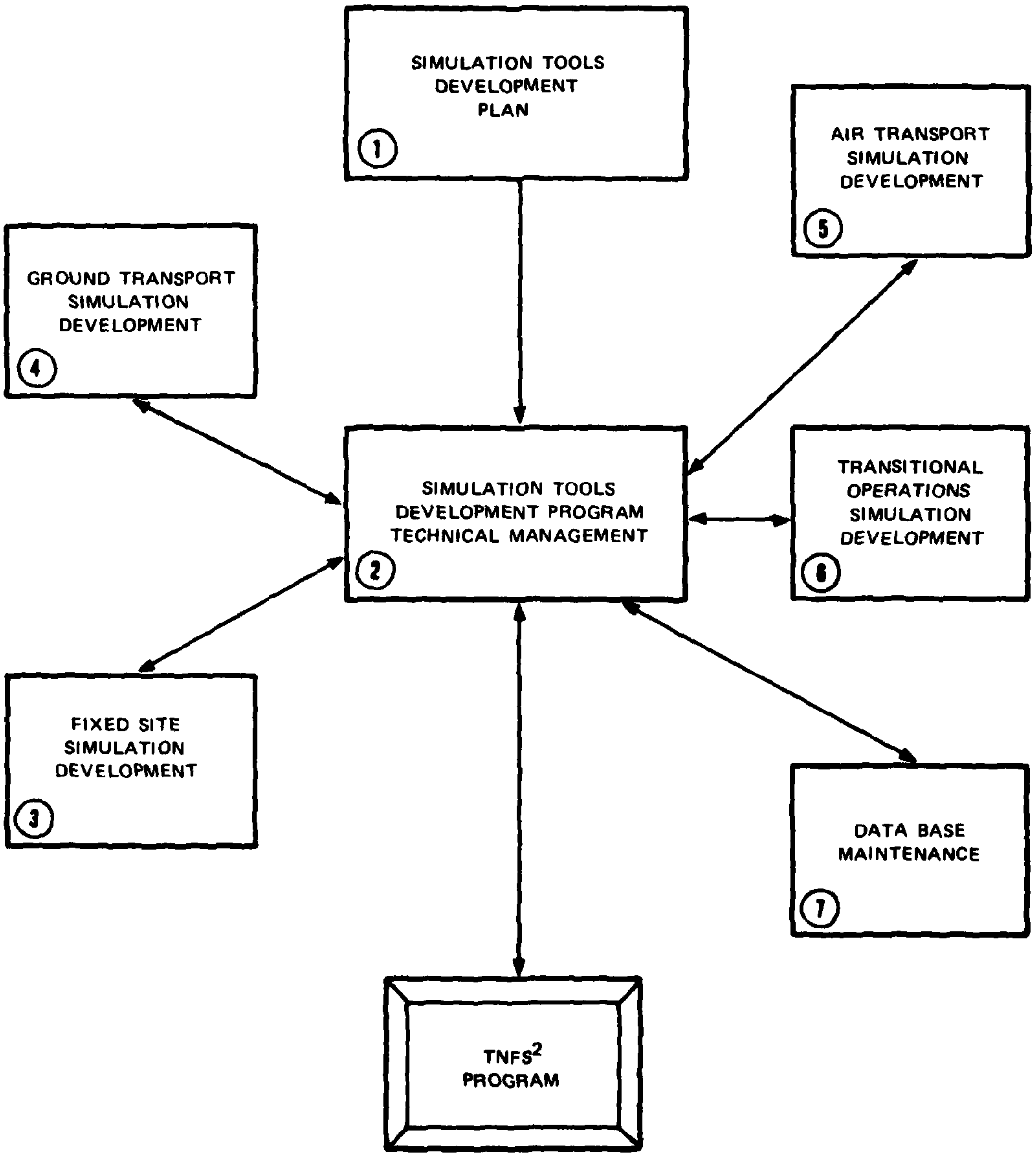
- The SOURCE/SABRES simulation combination developed by Sandia Laboratories is one set of simulations that is directly applicable to TNF security system evaluation, although some modification and expansion will be required.

- The TSEM (Transportation Safeguards Effectiveness Model) developed for Sandia Laboratories by the BDM Corporation is another simulation directly applicable to TNF security system evaluation requirements. Some modification will also be required.
- Most of the infantry combat simulations do not appear directly applicable for the TNFS$^2$ Program requirements. The SABRES and TSEM simulations make use of some of the better subroutines of these combat simulations.
- As an aggregated simulation, Schaffer's Ambush Model may be useful for TNF security system evaluation purposes. However, it would have to be broadly expanded for this purpose.

- Air Transport Simulations
  - No adequate simulation was uncovered that would be directly applicable for this case.
  - Most air-oriented simulations either are one-on-one simulations for evaluating air defense weapon effectiveness against fixed and rotary wing aircraft or are simulations for evaluating the effectiveness of attack helicopters in support of ground combat operations. However, some selected subroutines may be of use in the development of an air transport simulation for use in the TNFS$^2$ Program.

## Future Simulation Tools Development Program

Based on the results of the analysis, a seven-task simulation development program has been outlined. The first task is to establish a detailed plan for the development of the appropriate simulation tools to support the TNFS$^2$ Program. The second task is directed to all the activities required to provide technical management in the conduct of the simulation tools development program. The remaining five tasks are devoted to the actual development of the simulation tools and are broken down as follows: Fixed Site Simulation Development, Ground Transport Simulation Development, Air Transport Simulation Development, Transitional Operations Simulation Development, and Data Base Maintenance. The following figure indicates the interrelationship among these tasks.



SIMULATION TOOLS DEVELOPMENT PROGRAM--TASK INTERRELATIONSHIPS

# *PREFACE*

This report documents the analysis and findings of a research project conducted for the Defense Nuclear Agency, Washington, D.C. The technical monitor was Captain Jerome Bruni (USAF), FCPRT, of Defense Nuclear Agency, Field Command, Kirtland AFB, NM. The work was performed under Contract DNA 001-78-C-0321.

The research was performed in the Systems Evaluation Department (SED) of the Systems Research and Analysis Division (SRAD) of SRI International. Dr. Jacques Naar is Director of SED; Dr. David D. Elliott is Executive Director of SRAD.

Dr. Richard H. Monahan was the project leader and principal investigator. Edmund L. DuBois provided support in the areas of security system requirements and the threat. Dr. Lola Goheen and John H. Allen assisted in the evaluation of existing simulations.

CONTENTS

APPENDIX

## ILLUSTRATIONS

## TABLES

# SECTION 1

# INTRODUCTION

## 1.1 Purpose and Scope

The purpose of this research effort was to assist Defense Nuclear Agency (DNA) in its efforts to determine the simulation tools requirements in support of the Theater Nuclear Force Security and Survivability ($TNFS^2$) Program. This research effort involved an analysis of existing computer simulations to determine the availability of suitable simulations that could be used by DNA to evaluate the effectiveness of security systems and concepts in support of Theater Nuclear Force (TNF) weapons. The scope of this effort was restricted to peacetime security operations in the NATO theater of operations, although some consideration was given to the transition period from peacetime to open hostilities.

## 1.2 Background

A critical requirement imposed on NATO forces is the maintenance of the security of TNF weapons within NATO at various stages leading up to, and including, open hostilities between NATO and Warsaw Pact forces. During peacetime, most weapons are stored at sites that are presumably known to various adversary groups (Warsaw Pact forces, enemy agents, terrorist groups, and individual fanatics), and hence are prime targets for sabotage, pilfering, and disruptive rioting. Transport of TNF weapons during peacetime is also likely for the purpose of initial stockpiling of weapons and also for the transfer of weapons from one site to another for logistical or political reasons. Although these movements are generally conducted under secrecy, intelligent observers can detect abnormal activity that may indicate preparation for movement. Thus, the security of these weapons while in transport is particularly sensitive. In crises that could lead to open hostilities, movement of TNF weapons to dispersed field storage locations is likely, and this imposes an added burden on the NATO forces. During these periods, however, the troops would be in a high level of alert and stringent security measures would be in effect. At the onset of open hostilities, survivability of TNF weapons would become the primary objective, although security would still have to be maintained.

DNA is responsible for evaluating requirements designed to ensure that adequate procedures, material, and personnel are provided to maintain the security of TNF weapons in NATO Europe. Therefore, it is necessary to evaluate the effectiveness of alternative procedures, equipment, and personnel allocations as they relate to the maintenance and enhancement of the security of TNF weapons. One means of performing these evaluations is through simulation. Simulation analysis is an extremely useful and economical tool for evaluating a broad range of concepts and alternative systems under a variety of postulated environments. Thus, it is highly beneficial to DNA to determine the availability and usefulness of simulations that could be used in their security systems evaluations.

### 1.3 Method of Approach

The analysis was conducted in essentially four stages. The first stage involved a review of existing documentation and discussions with knowledgeable personnel to identify security system requirements in the protection of TNF weapons, to establish the threat spectrum of concern, and to establish a systematic representation of the kinds of events to which TNF weapons are subjected from arrival in the theater to their ultimate disposition. The results of this stage of the analysis are presented in Section 2 of this report.

The second stage of the analysis involved the identification of performance measures that would provide a quantitative basis for evaluating the effectiveness of existing or postulated security systems and concepts in maintaining the security of TNF weapons. The results of this stage of the analysis are presented in Section 3.

The third stage was directed to establishing how simulations could interface with testing to enhance the overall utility of the TNFS$^2$ Program. The results of this stage of the analysis are presented in Section 4.

The fourth stage of the analysis was concerned with the identification of simulations that could provide direct support to the TNFS$^2$ Program. The effort involved the conduct of a literature search to identify existing simulations that might be applicable to the support of the TNFS$^2$ Program and the subsequent detailed analysis of the selected simulations to determine their degree of applicability. The results of this stage are presented in Section 5.

Section 6 concludes this report with a description of a proposed program for future development of simulation tools to support the TNFS$^2$ Program.

## 1.4 Summary of Results

### 1.4.1 Security Requirements and Threat

The results of the analysis indicate the existence of stringent requirements on the security of TNF weapons. The guidelines call for security in depth, comprehensive physical and personnel security systems, use of deadly force if necessary, and frequent inspections, surveys, and certifications to ensure compliance. The threat spectrum extends from feints and demonstration probes to military assaults against nuclear weapons in storage or in transit by small to large groups of fanatics, terrorists, or military forces. Attackers will use whatever means are available to achieve their objective, capitalizing on surprise, diversion, deception, confusion, ambush, speed and shock effect. The threat objectives range from peaceful demonstrations and disorderly disruptions on up through hostile attempts at sabotage or theft.

### 1.4.2 Performance Measures

The overall objective of a security system for theater nuclear weapons not only includes the protection of these weapons from damage, destruction, or diversion, but also the avoidance of any incidents, intended or not, whose direct or indirect effects could have noticeable political repercussions or could lead to hostile actions. Because of the diverse nature of these possible situations that could result in a nuclear accident or incident, the establishment of a single, broad performance measure to be used in evaluating and comparing effectiveness of security systems and improvements thereto would not prove fruitful in the long run. A more useful approach is to adopt performance measures that address the different functional aspects of a security system, represented by dissuasion, detection, assessment, communication, delay, and neutralization. This is particularly advantageous in supporting a test program where many of the tests would fall totally within the jurisdiction of a single functional area. Furthermore, more aggregated performance measures, if required, could be obtained from the functional area performance measures by relatively simple algebraic or probabilistic computations.

### 1.4.3 Simulation/Testing Interface

Computer simulations, if properly designed and applied, can be extremely valuable tools to be used in support of test programs directed at evaluating the effectiveness of TNF security systems under operational conditions. The constraints of both time and cost impose severe limitations on the amount and scope of testing that can be conducted. Furthermore, certain facets of security system operations are untestable due to safety considerations. With proper planning, simulations can expand the scope and depth of the evaluation process in addition to providing valuable insights for use in test planning. Testing, on the other hand, can enhance the credibility of simulation outputs by providing near-real-life results that can be used for simulation validation and/or calibration. Thus, simulation and testing can interact synergistically with one another to provide for a broad-based, efficient evaluation program. In order to be of useful assistance in the conduct of a testing program, simulations should possess the characteristics of completeness, modularity, test compatibility, machine independence, and usability. To satisfy the completeness characteristic, a single simulation covering all the confrontation situations for weapons at fixed sites, in ground transport, in air transport, or in transition between two of these weapon status states would probably be so large as to violate the usability characteristic. Thus, it is likely that a set of simulations, each covering one of the weapon status state conditions, would prove more efficient in the long run. An additional desirable, though not necessary, characteristic is dual complexity, which refers to the availability of an aggregated and a detailed simulation for each functional area.

### 1.4.4 Availability of Simulation Tools

A literature search was conducted to identify those simulations that might be applicable for use in support of the $TNFS^2$ Program. Over 1100 abstracts were identified and an initial screening of these abstracts resulted in the obtaining of 129 reports that appeared relevant to the purposes of this analysis. A cursory review of these reports resulted in the identification of 41 simulations that could have direct applicability. These were reviewed in more depth and ten simulations were determined to have some direct application in providing support to the test program. These were grouped into three sets (fixed site simulations, ground transport simulations, and air transport simulations) and subjected to detailed analysis. No simulation appeared to directly address any of the transitional operations. The results of this analysis led to the following general conclusions:

- Simulations developed for purposes other than security system evaluation are not, in general, easily adaptable for the purpose of security system evaluation.
- Simulations developed for the purpose of security system evaluation do provide an adequate base for the development of TNF security system evaluation simulations.
- The simulations reviewed are directed to a single weapon status state (fixed site, ground transport, or air transport) and thus do not address the transitional operations involved in going from one state to another.
- For the purposes of the $TNFS^2$ Program, a significant amount of simulation development activity will be required.

- Sandia Laboratories has amassed a broad security system data base that will be of use for the TNFS$^2$ Program.
- Fixed site and ground transport simulations are available that can be built upon to satisfy the requirements for support to the TNFS$^2$ Program.
- No adequate air transport simulation was uncovered that would have direct applicability to the requirements for support to the TNFS$^2$ Program.

### 1.4.5 Future Simulation Tools Development Program

Based on the results of the analysis, a seven-task simulation development program has been outlined. The first task is to establish a detailed plan for the development of the appropriate simulation tools to support the TNFS$^2$ Program. The second task is directed to all the activities required to provide technical management in the conduct of the simulation tools development program. The remaining five tasks are devoted to the actual development of the simulation tools and are broken down as follows: Fixed Site Simulation Development, Ground Transport Simulation Development, Air Transport Simulation Development, Transitional Operations Simulation Development, and Data Base Maintenance.

# SECTION 2

# SECURITY REQUIREMENTS, THREAT, AND NUCLEAR WEAPON EVENTS*

## 2.1 Security

The policy guidelines established by the Department of Defense for the security of nuclear weapons call for security in depth; for comprehensive physical and personnel security systems; for the use of every means available to ensure security (including deadly force if necessary); for compensatory measures to maintain standards whenever circumstances mandate waiver or exception to established criteria; and inspections, surveys, and certifications to ensure compliance. The policy does explicitly correlate nuclear weapon protection requirements with the threat existing at any time: An increased threat dictates an increase in security measures. In this respect, the policy establishes security requirements--over and above mandatory minimum requirements--in proportion to the threat.

In response to the broad policies and requirements established by the Office of the Secretary of Defense, standards, criteria, procedures, and equipment to ensure nuclear weapon security are specified by the Military Departments and field commands in great detail. It is, of course, not necessary to draw upon all of this detail to derive security system performance measures and simulation requirements. The elements that comprise the current security program and the general nature of the standards, criteria, and methods do, however, provide a basis for assessing how simulations may be applied to evaluate system improvement. It is to be expected that the philosophy and principles--and much of the detail--of the security program as currently promulgated will remain valid despite future changes in theater nuclear posture.

*References 1 through 24 (listed at the end of this report) provided most of the background material for this section. Although some additional classified references were consulted in order to obtain a complete understanding of nuclear weapons security operations, no classified material was used in preparing the material appearing in this report.

The following characteristics of the current security program are particularly noteworthy:

- The requirement for security in depth involves multiple, redundant, and sequential safeguards of all kinds. This extends to barrier systems, warning systems, communication systems, personnel behavioral safeguards, security forces, and other aspects. The categories of restricted, limited, and exclusion areas prescribed around nuclear weapons at all times* and the graded access and human reliability controls applied to these controlled areas reflects the principle of sequential safeguards in depth.
- There are careful controls under the Personnel Reliability Program to guard against aberrant behavior of personnel who may have access to or knowledge of nuclear weapons. This starts with selection and training of entry personnel and is continued thereafter for all persons associated with or influencing nuclear weapon security. Despite this carefully structured system, there may be difficulties in motivating guard personnel.
- Strict inspections, security surveys, and certification of facility, equipment, transportation adequacy, and personnel proficiency and reliability ensure that criteria are met, and also provide one means of measuring the effectiveness of the existing system.
- The system explicitly guards against both inadvertent and intended breaches of security. The two-man concept to protect against incorrect or unauthorized procedures is rigidly applied as one means to guard against both inadvertent and deliberate acts that could degrade weapon performance. Other controls of the human element include control of technical knowledge of and access to nuclear weapons.
- The concept of continuous U.S. custody is strictly adhered to up to the time possession is transferred to designated non-U.S. delivery units in accordance with Presidential authorization. Continuous accountability as to disposition is maintained even after transfer to custody and possession.
- Major reliance is placed on physical security means, but in no case is sole reliance placed on physical security without human backup. When physical barriers are impractical, other means with comparable effectiveness must be used. Permissive action links (PAL) function as a command-control element to ensure Presidential control of weapons, but they also can serve as a last-ditch physical barrier, thus adding to security.

*Even during movement an exclusion area around nuclear weapons is maintained.

- Security requirements now extend to protection from electromagnetic radiation environments that could affect physical security equipment and nuclear weapons themselves. Increased concerns about Soviet and Warsaw Pact electronic warfare capabilities add to the importance of guarding aginst this threat to security.

- Survivability, security, and reliability of control and communications systems supporting theater nuclear forces have also been subjects of concern in recent years. Communication system requirements are established for all echelons down to storage sites and for the movement of weapons.

- Movement of nuclear weapons is to be kept to the minimum consistent with operational requirements. Nevertheless, short-distance ground movements and longer-distance air movements are a frequent occurrence. Routine and emergency procedures, guard forces, movement planning, vehicle inspection and certification, communications, and other requirements are spelled out in detail.

- Presently, the preferred mode of transportation of nuclear weapons is by air. However, the threat of man-portable ground-to-air precision weapons in the hands of terrorist organizations could conceivably force a shift away from air movement in favor of ground movement for both short and long hauls. Moreover, in situations where large numbers of nuclear weapons are dispersed to field storage, ground movement may be the normal means of transportation if helicopter resources prove to be inadequate to handle the volume of traffic.

- The DoD requirements to use every means available to safeguard weapons are explicit. The fact that deadly force is to be used where necessary, including situations where hostages have been taken, is indicative of the seriousness attached to the security mission. This policy, if known to terrorist groups, could be an important deterrent to terrorist actions that depend for success upon the taking of hostages. DoD requirements also call for emergency evacuation or emergency destruction capability where protective measures fail.

- Actions to be followed in case of nuclear accident or incident are specified in considerable detail under the Nuclear Accident and Incident Control (NAIC) Program. The accidents and incidents of concern include those that happen inadvertently and those caused deliberately. Breaches of security and attempted breaches are themselves defined as accidents or significant incidents. Since nuclear accidents and incidents immediately interrupt the normal sequence of weapon events, the possibility arises that a minor incident might intentionally be created in order to set the stage for a more serious follow-up action by a hostile group.

- Although the basic principles of full security continue to apply under combat conditions, requirements take into account the different perspectives that apply in wartime. In particular, there is a clear differentiation between requirements pertaining to logistical movement of nuclear weapons and movement in a tactical environment. Commanders are allowed to deviate from requirements as necessary to conform to the tactical environment.
- An important aspect of security requirements is the importance attached to correct interpretation of the intent and temper of any suspected or attempted breach of security. This is necessary to guard against using excessive force in response to innocent trespassing or encroachment, but equally important, is essential for timely, adequate response to fast-moving events in an intended forceful breach.

## 2.2 Threat

Under conditions of peace and crisis, threats to the security of nuclear weapons in Europe and other overseas theaters include both inadvertent and deliberate actions, and can arise from the actions of persons who are ostensibly friendly and persons who are openly hostile. Although there does not appear to be evidence of a significant increase in subversive activities against military elements by individuals acting alone, there is abundant, well-documented evidence of an increase in overt and covert actions by organized groups against institutions of society and government, including military elements. In particular, the marked upsurge over the past two decades in organized international and transnational terrorism constitutes a very serious threat to military establishments.

There does not seem to be a basis for expecting that this threat will abate in the near future. It may well increase, especially from groups that depend on their own resources rather than on support by sovereign nations. In addition, the Soviet Union clearly has the capabilities to initiate or sponsor forceful actions against nuclear weapons and forces. It is known that Soviet tactics specifically include nuclear weapons and forces as priority war targets. The use of special forces or airborne forces by the Soviet Union (or other East European countries) in clandestine operations is a capability that could be seriously detrimental.

The individuals and organizations that can constitute threats in peacetime and crises include:

- Psychologically or emotionally disturbed individuals assigned to nuclear weapon duties.
- Individual fanatics, with political leanings either to the right or the left.
- Overt political antinuclear and antimilitary dissident groups.
- Organized crime and other criminal elements.
- Radical national political groups.
- International and transnational terrorist organizations.
- Military forces of a disaffected ally or insurgent military forces of a loyal ally.
- Intelligence organizations of adversary nations.
- Adversary special forces.
- Adversary air, airborne, and air assault military forces.

The actions these threat elements might take against nuclear weapons range from overt nondestructive demonstrations (such as by dissident political groups) to covert destructive and nondestructive actions of many kinds, to direct surprise assaults. The threat objectives can be nonviolent and nondestructive or can be destructive and violent, including the taking of hostages. Objectives can encompass any one or combination of the following:

- Hoax.
- Publicity for a political cause.
- Political embarrassment of the United States or its allies.
- Ransom for a political purpose.
- Ransom for money.
- Revenge.
- Espionage.

- Sabotage.
- Acquisition for use in future terrorist action.
- Takeover by an ally for political purpose or for unilateral military use by its forces in conflict.
- Direct military action by an enemy as the prelude to hostilities.

The extreme political sensitivity attached to nuclear weapon security tends to lower the threshold of threat actions that constitute serious security incidents. Thus a forceful demonstration of capability to penetrate a nuclear security system, even if not carried to the point of actual penetration, can be a useful objective for a group seeking a political aim and a serious erosion of public confidence in security effectiveness. Likewise, an action that physically endangers a nuclear weapon--such as launching a missile against an aircraft or a truck carrying nuclear weapons--might lead to serious political perturbations and gain a terrorist organization needed publicity on a worldwide scale, even if no harm to the weapons results. This potential for leveraging what would be minor threat incidents with most weapons into major threat incidents when nuclear weapons are involved magnifies the problem facing the nuclear weapon security system.

By the same token, more serious actions such as damage, detonation, or capture of a weapon or weapon component can become prime objectives for terrorist political purposes out of all proportion to the imminent danger to U.S. national security. If a single action of this kind is carried out with even limited success, there might well be such severe political reactions by the United States or its allies that theater nuclear force readiness could be reduced by the resulting inhibiting constraints. Security system effectiveness must be measured by its ability to guard against only partially successful breaches and demonstrations of security weakness as well as more destructive actions.

At the other end of the spectrum of peacetime and crisis security threats are military or paramilitary operations on a larger scale intended to influence the political climate or to degrade U.S. national security. Soviet attention to the offensive and to the importance of decisive initiative in attacking enemy nuclear weapon systems indicates that the peacetime security system may have to cope as the first line of defense against a surprise airborne and airmobile assault immediately preceding overt hostilities.

Whether fanatic or terrorist or military force, the attacker will depend on surprise, diversion, deception, confusion, ambush, speed, and shock effect. Enough can be learned by threat organizations about nuclear security activities, patterns, storage locations, guard force size, weapons, and barriers to provide a basis for attack planning and timing. Modern weapons such as man-portable homing missiles, smoke agents, chemical agents, and laser guided weapons can be acquired and used.

In summary, the threat spectrum extends from deints and demonstration probes to military assaults against nuclear weapons in storage or in transit. The likelihood, and the impact if initiated, of any of these threat actions is serious enough that the security system (augmented as necessary) must show itself able to protect weapons against the full spectrum without sacrificing readiness. By testing and measuring the security system, its effectiveness can be established and the confidence of political and military authorities in the system maintained.

## 2.3 Nuclear Weapon Events

To facilitate development of performance measures and provide a framework for considering the utility of simulations, the kinds of events to which nuclear weapons are subjected from arrival in theater to disposition are listed in Table 2.1. Table 2.1 also lists events that relate to nuclear storage sites rather than to the weapons themselves. These events can have an impact on the security of nuclear weapons. Since there can be wide variations in the particular circumstances under which each of the listed events occurs, further detailing of events will be necessary for assessing the utility of candidate simulations.

Flowcharts showing the sequence of weapon events from Table 2.1 are presented in Figures 2.1, 2.2, and 2.3. Figure 2.1 depicts weapon movement event sequences that may occur during the normal in-theater lifetime

Table 2.1

IN-THEATER NUCLEAR WEAPON EVENT CATEGORIES

A. Aircraft Transportation Events

A1 On-loading operations

A2 Air movement (into theater airbase from CONUS or another theater, within theater to another airbase, or out to CONUS or another theater)

A3 Airbase arrival and off-loading operations

A4 Weapon reception activities (including inventory and inspection) at airbase

A5 Local Movement on airbase

A6 Temporary in-transit storage at airbase

B. Helicopter Transportation Events

B1 On-loading operations

B2 Air movement

B3 Heliport arrival and off-loading operations

B4 Weapon reception activities at heliport

C. Ground Transportation Events

C1 On-loading operations

C2 Ground movement

C3 Arrival at destination and off-loading operations

C4 Weapon reception activities at destination (storage location, heliport, or airbase)

D. Storage Events

D1 Local movement on site

D2 Temporary storage outside protected storage structures at fixed sites

D3 Storage in protected storage structures at fixed or quick-reaction alert (QRA) site

Table 2.1 (Concluded)

D. Storage Events (continued)

| | |
|---|---|
| D4 | Field storage at a NATO atomic supply point (NASP) or a special ammunition supply point (SASP)* |
| D5 | Field storage at non-QRA delivery unit |
| D6 | Field storage on QRA aircraft or Pershing missile |
| D7 | Weapon maintenance activities |
| D8 | Preparation for weapon employment |
| D9 | Weapon expenditure |

E. Nuclear Incident and Accident Events

| | |
|---|---|
| Elmi | Minor incident |
| Elsi | Significant incident |
| Elac | Accident |
| Elwr | War risk accident |
| E2 | Initial inspection |
| E3 | Movement interruption (aircraft or helicopter landing, ground convoy halt) |
| E4 | Off-loading and temporary storage |
| E5 | Detailed inspection and remedial actions, including local security measures |
| E6 | Disposition action (other than emergency destruction) |
| E7 | Emergency destruction |

F. Non-Weapon Site-Related Events

| | |
|---|---|
| F1 | Site visits by military and government personnel |
| F2 | Site access by civilian maintenance personnel |
| F3 | Site non-weapon maintenance and repair activities |
| F4 | Site construction and upgrading activities |
| F5 | Site participation in training exercises involving external units |
| F6 | Site participation in nonweapon training not involving external units |

*NASP and SASP are essentially synonomous terms for a field storage location (FSL) operated by an ordnance direct support unit. It is usually fully mobile, but may be semimobile. An FSL is any nonpermanent, nonfixed storage location to which nuclear weapons are dispersed under tactical conditions from fixed storage sites.

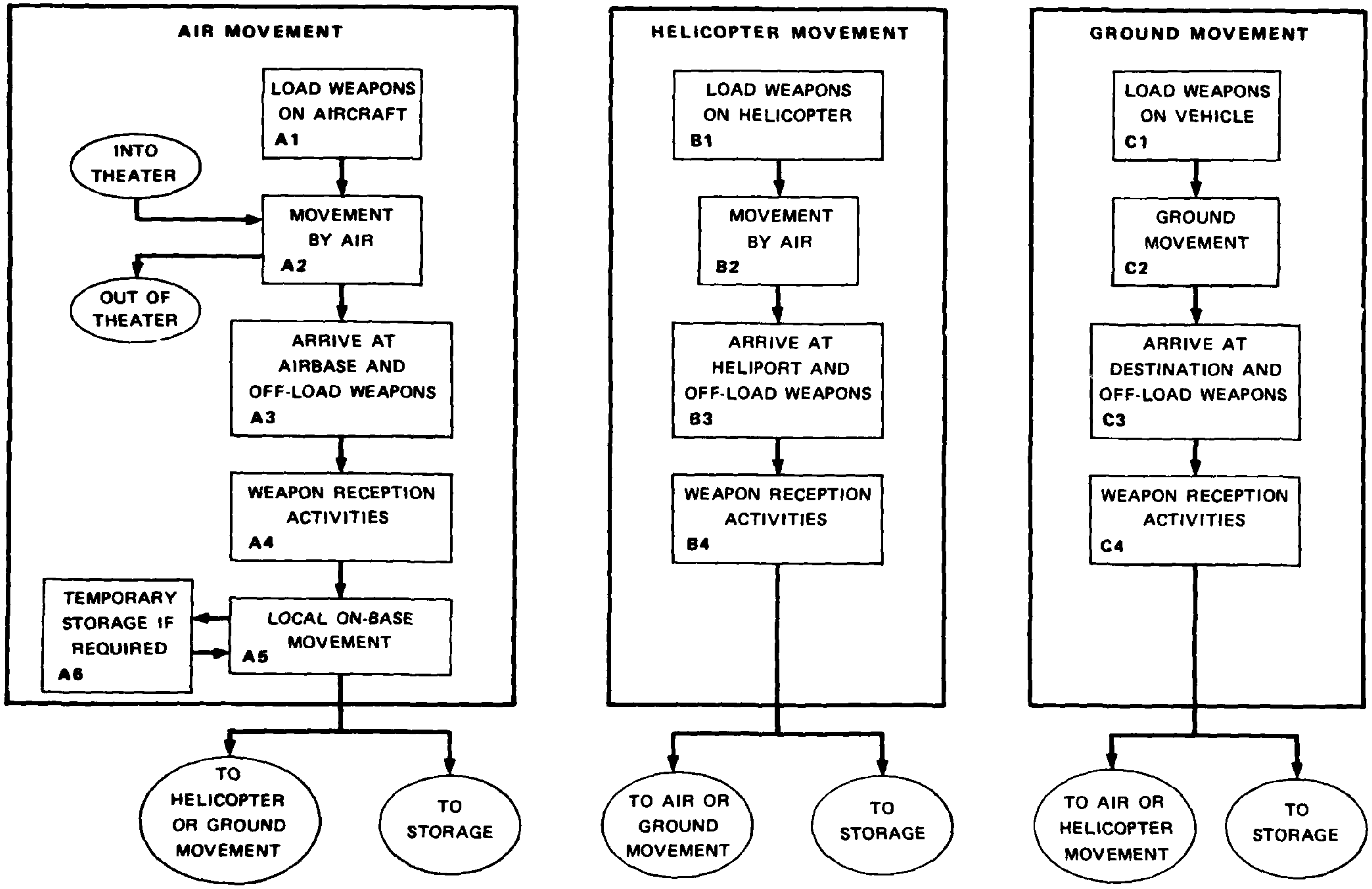

AIR MOVEMENT
LOAD WEAPONS ON AIRCRAFT A1
INTO THEATER
MOVEMENT BY AIR A2
OUT OF THEATER
ARRIVE AT AIRBASE AND OFF-LOAD WEAPONS A3
WEAPON RECEPTION ACTIVITIES A4
TEMPORARY STORAGE IF REQUIRED A6
LOCAL ON-BASE MOVEMENT A5
TO HELICOPTER OR GROUND MOVEMENT
TO STORAGE
HELICOPTER MOVEMENT
LOAD WEAPONS ON HELICOPTER B1
MOVEMENT BY AIR B2
ARRIVE AT HELIPORT AND OFF-LOAD WEAPONS B3
WEAPON RECEPTION ACTIVITIES B4
TO AIR OR GROUND MOVEMENT
TO STORAGE
GROUND MOVEMENT
LOAD WEAPONS ON VEHICLE C1
GROUND MOVEMENT C2
ARRIVE AT DESTINATION AND OFF-LOAD WEAPONS C3
WEAPON RECEPTION ACTIVITIES C4
TO AIR OR HELICOPTER MOVEMENT
TO STORAGE

FIGURE 2-1 NUCLEAR WEAPON MOVEMENT EVENT SEQUENCES

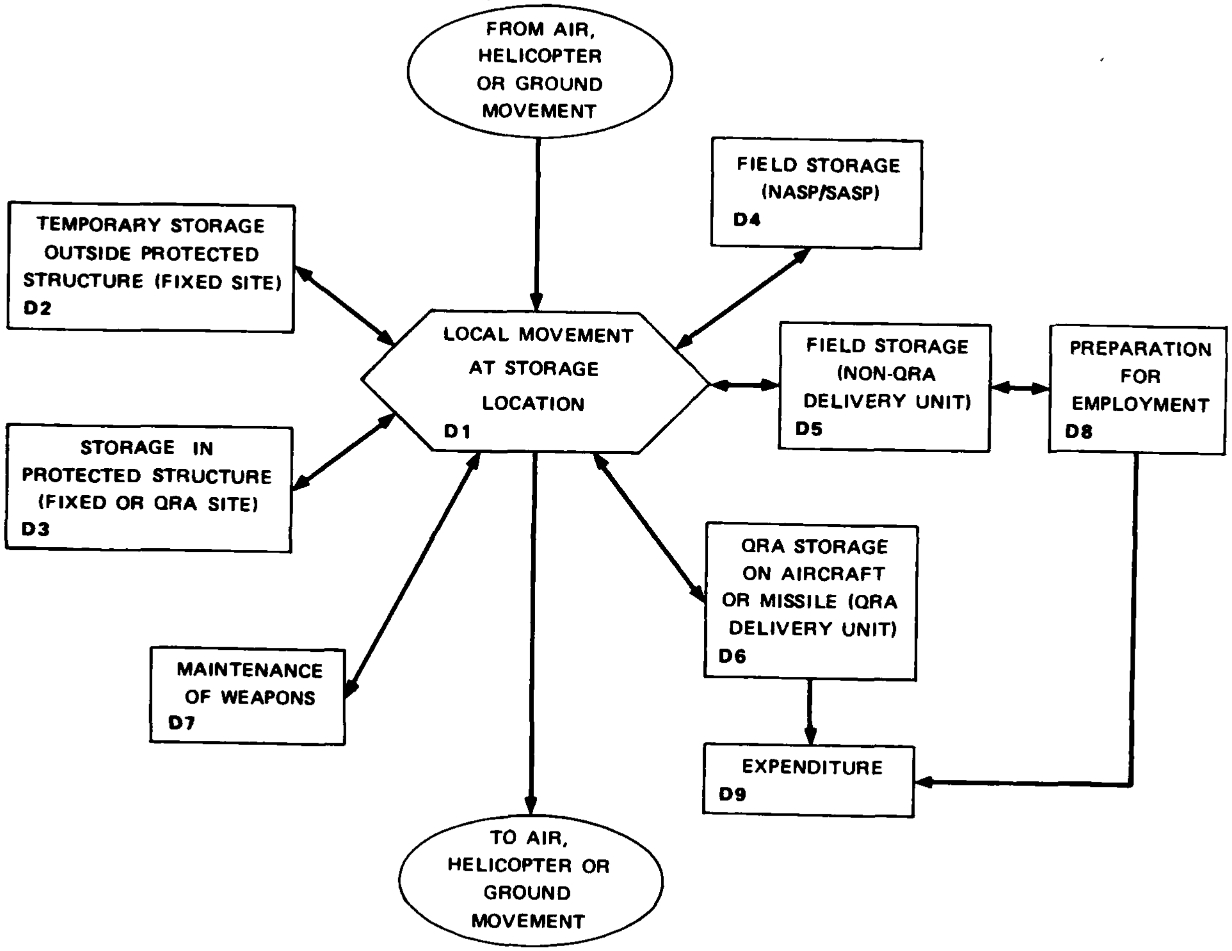

FROM AIR, HELICOPTER OR GROUND MOVEMENT
TEMPORARY STORAGE OUTSIDE PROTECTED STRUCTURE (FIXED SITE) D2
FIELD STORAGE (NASP/SASP) D4
LOCAL MOVEMENT AT STORAGE LOCATION D1
FIELD STORAGE (NON-QRA DELIVERY UNIT) D5
PREPARATION FOR EMPLOYMENT D8
STORAGE IN PROTECTED STRUCTURE (FIXED OR QRA SITE) D3
QRA STORAGE ON AIRCRAFT OR MISSILE (QRA DELIVERY UNIT) D6
MAINTENANCE OF WEAPONS D7
EXPENDITURE D9
TO AIR, HELICOPTER OR GROUND MOVEMENT

FIGURE 2-2 NUCLEAR WEAPON STORAGE EVENT SEQUENCES

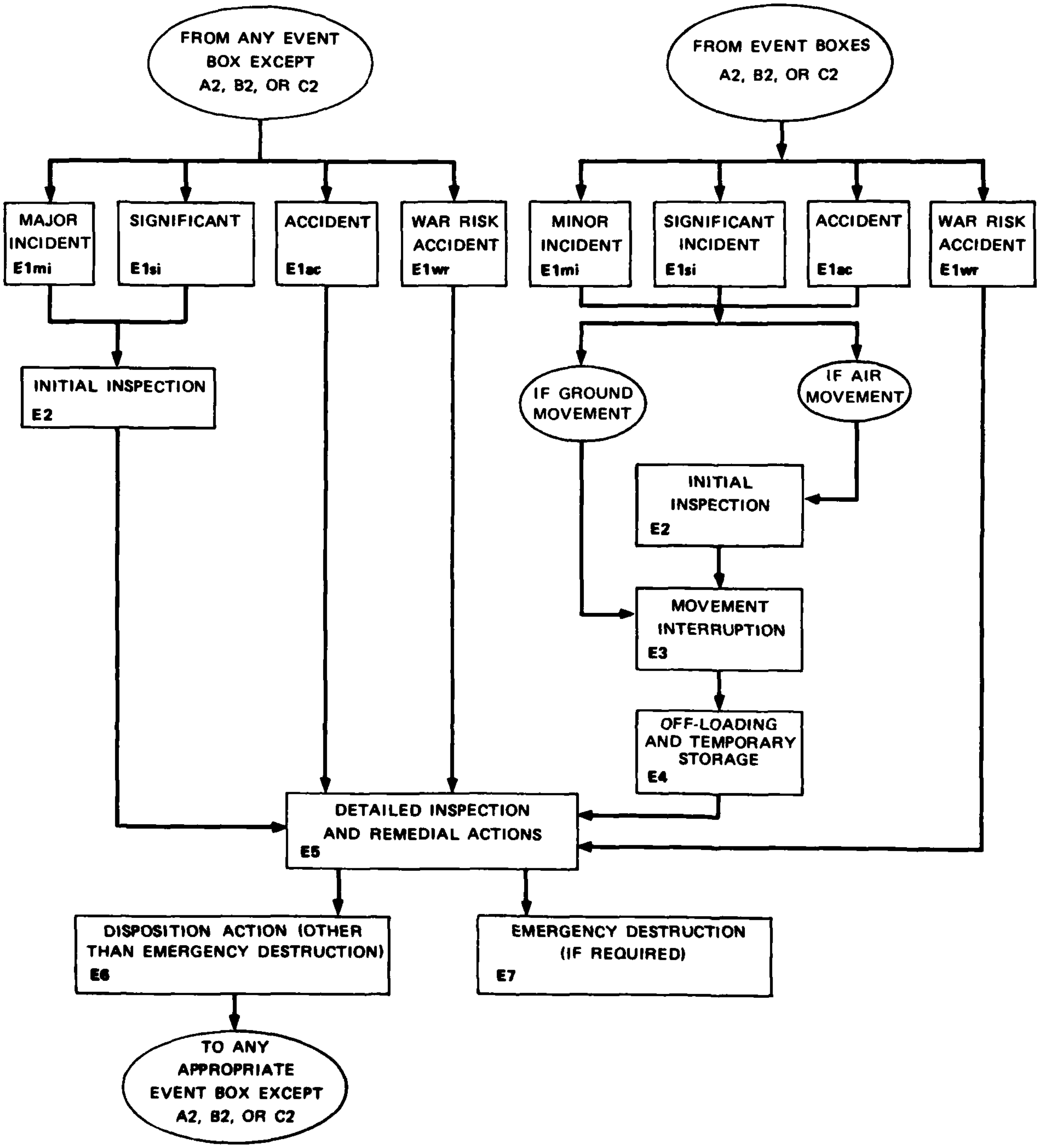

FROM ANY EVENT BOX EXCEPT A2, B2, OR C2
FROM EVENT BOXES A2, B2, OR C2
MAJOR INCIDENT E1mi
SIGNIFICANT E1si
ACCIDENT E1ac
WAR RISK ACCIDENT E1wr
MINOR INCIDENT E1mi
SIGNIFICANT INCIDENT E1si
ACCIDENT E1ac
WAR RISK ACCIDENT E1wr
INITIAL INSPECTION E2
IF GROUND MOVEMENT
IF AIR MOVEMENT
INITIAL INSPECTION E2
MOVEMENT INTERRUPTION E3
OFF-LOADING AND TEMPORARY STORAGE E4
DETAILED INSPECTION AND REMEDIAL ACTIONS E5
DISPOSITION ACTION (OTHER THAN EMERGENCY DESTRUCTION) E6
EMERGENCY DESTRUCTION (IF REQUIRED) E7
TO ANY APPROPRIATE EVENT BOX EXCEPT A2, B2, OR C2

FIGURE 2-3 NUCLEAR ACCIDENT AND INCIDENT EVENT SEQUENCES

of weapons. Many of the event sequences are, of course, repetitive. Figure 2.2 depicts normal sequences of events that occur while weapons are at fixed or field storage locations, including preparation for employment and expenditure of weapons in combat. Figure 2.3 depicts event sequences that arise whenever a nuclear accident or incident occurs. These represent abnormal temporary diversions that interrupt the normal progression of events shown in Figures 2.1 and 2.2. An accident or incident could occur while any of the events in Figures 2.1 and 2.2 is in process. Any actual or attempted penetration or other unexpected degradation of nuclear weapon security is classed as, at least, a "nuclear weapon significant incident" (Event Elsi). If the event results in certain more serious situations, such as a weapon detonation or seizure, it is classed as a "nuclear weapon accident" (Event Elac) or a "nuclear war risk accident" (Event Elwr).

# SECTION 3

# PERFORMANCE MEASURES

## 3.1 General

The overall objective of the total security system for theater nuclear weapons is to maintain the security of the weapons--that is, to ensure the prevention of the occurrence of a nuclear accident or incident relative to these weapons. This includes not only the protection of theater nuclear weapons from damage, destruction, or diversion, but also the avoidance of any incidents, whether intended or not, whose direct or indirect effects could have noticeable political repercussions or could lead to hostile actions. Thus, any measure of the overall performance capabilities of a security system should be directly related to the probability of occurrence of nuclear accidents or incidents over some broad time span.

The use of such a broad measure in comparing alternative security systems or concepts, or in evaluating the effects of improvements to a given system, would require the establishment of a hypothetical base-case scenario of action-inducing events that would serve as a standard for the measurement of overall security system performance. This base-case scenario could take the form of a series of abnormal events at specific times within a specified time period, or it could be in terms of a probability distribution over a set of abnormal events that might occur within the specified time period. The difficulty in establishing a scenario that would be universally accepted within the defense community is one of a number of drawbacks in utilizing such a broad performance measure as specified above. Another drawback is such a scenario's lack of sensitivity to a system's performance relative to an extremely unlikely (but possible) event, the result of which could have dire repercussions. Furthermore, system improvements generally address specific flaws in the system that may only affect performance against a small subset of action-inducing events, and only produce negligible changes in the broad performance measure, which is tied to a multitude of such events. Since the TNFS$^2$ Program as presently structured is directed toward improvements in selected aspects of the present security system, it is apparent that the use of such a broad performance measure would not be useful for many of the program's objectives.

In view of the above, a more fruitful approach is to adopt performance measures that address the different functional aspects of a security system. One such approach is to consider five basic functions of a security system (detection, assessment, communication, delay, and neutralization) and establish appropriate performance measures for each of these functions. This approach was adopted by the Sandia Laboratories in their work under the SAFEGUARDS program for the Nuclear Regulatory Commission (NRC). This method allows comparisons of specific changes. In addition, with properly chosen performance measures, the method can provide an appropriate base for more aggregated performance measures through relatively simple algebraic or probabilistic computational procedures. One additional function should, however, be added to the five used in the Sandia Laboratories approach: The important dissuasive aspects of a security system--that is, the attributes that discourage the initiation of attempts to breach the system. Included in this function are the deterrent aspects inherent in a seemingly impregnable security system and the secretive aspects of withholding information relative to weapon storage locations and pending movements of weapons. Dissuasion can be, in itself, an extremely important function of security system. As such, it should be considered in measuring the performance characteristics of security systems.

The approach adopted for this analysis is based on the establishment of performance measures for the following six basic functions of a security system: dissuasion, detection, assessment, communication, delay, and neutralization. Candidate measures for these functions are discussed in the following subsection.

### 3.2 Candidate Performance Measures

The performance measures listed in this subsection represent a set that would be useful in evaluating modifications to security systems and concepts or in comparing alternative security systems. Whether or not reliable estimates for these performance measures can be obtained through simulation is not addressed here. The presentation that follows considers performance measures for each of the six functions in turn. For each function, multiple performance measures are identified. In some cases this is due to the general nature of the function. In other cases a function may have different aspects, depending on the status of the weapons--that is, whether or not the weapons are stationary (permanent or temporary storage), in transit by air (fixed-wing or helicopter), or in transit by ground (local or long distance).

3.2.1 Dissuasion is the most difficult of the six security system functions for which to establish useful performance measures. The two subfunctions of dissuasion (deterrence and secrecy) are each difficult to quantitatively portray. Deterrence is basically psychological in nature, and any direct measure would therefore necessarily be highly subjective, depending in a large part on the risk-acceptance attitudes of each particular adversary group considered in the threat spectrum. The risk function, if expressed in terms of expected losses to be incurred by an adversary group, however, is a measurable function and can serve as an indirect measure for deterrence. That is, the higher the risk to an adversary, the less likely will be his desire to attempt to breach the security system. Thus, one candidate measure for the deterrence aspect of dissuasion is the expectation by an adversary of losses to be incurred, given an attempt to breach the security system. In some cases, risk may not be a deciding factor, and an alternative criterion may be derived from the cost or value of resources required to assure a certain level of success. Here an alternative candidate measure could be the minimum adversary resource value required to assure a specified probability of success. These two deterrence performance measures are applicable regardless of whether weapons are in storage or in transit.

The secrecy subfunction of dissuasion considers the function of a defender's counter-intelligence activities in denying an adversary information concerning weapon storage locations, movement plans, and security measures. For weapons in storage, the principal performance measure is the probability that an adversary group has timely knowledge of the weapon storage location. The time element included in this measure is more applicable to temporary storage, but could apply to permanent storage in cases where weapons are subjected to occasional relocations within the site or between sites. For in-transit cases, a prerequisite for an intentional breach attempt by an adversary is prior knowledge of certain aspects of the movement events. Thus, the principal performance measure for these movement cases is the probability that an adversary group has timely knowledge of movement events. Since movrment will normally require temporary storage at each end of the movement, the two performance measures above will obviously be tied together for these cases. For both of these performance measures, timeliness is a critical modifying parameter in that an adversary must have sufficient lead time to plan his tactics, assemble personnel and equipment, and emplace his forces in such a manner as to ensure a high probability of successful attack at the proper time.

### 3.2.2 Detection

The detection function is a necessary prerequisite for employment of active security measures. Detection in itself is important only if the security system elements have adequate time to react sufficiently to neutralize the adversary force and avoid the occurrence of a nuclear accident or significant incident. Thus, the timeliness of detection is tied to the available reaction time.

For weapons in a stationary status (permanent or temporary storage), available reaction time can be directly related to the depth remaining for the adversary to penetrate at time of initial detection. Hence, an important performance measure for these cases is the cumulative probability of initial detection as a function of the depth remaining to penetrate. In some cases this depth may be specified as a continuous distance function, while in other cases it may be specified by discrete points that signify the locations of barriers, protective zone boundaries, storage igloo entrances, etc. Although initial detection of an adversary is the primary factor, secondary detections at various points along an adversary action path will also be of concern. Thus, subsidiary performance measures could include the probability of detection at specific checkpoints given a prior initial detection.

For weapons in transit, the important performance capability is the ability to detect the presence of adversaries prior to the initiation of hostile actions. This prior detection will certainly negate the surprise element of the impending confrontation, will allow more time for reinforcement by back-up forces, and may even be sufficient to allow avoidance of a confrontation through alternate routing. For these cases, then, a useful performance measure would be the cumulative probability of detection as a function of the time prior to an imminent confrontation. The time variable may either be a continuous function or be specified as discrete time intervals reflecting, say, minimum required reaction time and minimum required confrontation avoidance time.

For detection mechanisms that issue an alarm prior to assessment, the false alarm rate is also a performance measure to be considered. Other false detection situations are covered under the assessment function.

### 3.2.3 Assessment

The assessment function involves the analysis of detection information to determine if, indeed, responsive action is required, and if it is, to determine the proper response to be taken. Of primary importance when an adversary action is taking place is the time required to make an assessment and decide on a response. Thus, the assessment delay time is an important performance measure to be considered. Depending on the level of analysis, this may take the form of an expected valu , possibly conditioned on whether or not an adversary action is indeed in progress, or it may be expressed in more detail as a probability distribution. Of equal importance is the probability of making a correct assessment, especially when the adversary action is such that an incorrect assessment could be disastrous. When an adversary action is not taking place, a so-called detection could be correctly assessed (nuisance detection) or incorrectly assessed (false alert). Both of these conditions, especially if frequently occurring, can degrade the effectiveness of a security system, so that the false alert rate and nuisance detection rate are both also measures that may be of concern. One special case of a false alert that can be very important is when the false assessment results in excessive force being brought to bear on an inadvertent or peaceful intruder. (This case is covered again under the neutralization function.) The performance measures indicated above are applicable when the weapons are stationary or in transit, although in the latter case correct assessment may be near-instantaneous when detection is triggered by the initiation of a hostile adversary confrontation.

### 3.2.4 Communication

The communication function is concerned with informing the security forces (local and/or back-up) that an adversary action is taking place or is imminent. Of primary importance is the time required to alert security forces under these conditions. Hence, a useful performance measure is the communication delay time, which can be expressed either as an expected value or as a probability distribution. Of equal importance is the probability that the minimum required information is received (by the intended recipient). The "minimum required information" as used here implies that correct interpretation of the information received (possibly incomplete or partially erroneous) would result in the recipient taking the right action required by the content of the original message. The performance measures identified in this section apply to both stationary and in-transit.

It should be noted here that assessment and communication are not "one-shot" functions, but must be continually in force subsequent to the initial detection assessment and communication of information to the security forces. This, of course, represents the $C^3$ aspects of the security force and would be included in the factors contributing to the security force's ability to neutralize the adversary.

### 3.2.5 Delay

The delay function encompasses all activities that slow or stop an adversary in the performance of his desired mission. This includes delays attributable to barriers (passive or active) and to the presence and actions of security forces (local and back-up). Delays affect the security system performance in two respects: (1) Predetection delay enhances the probability of detection by increasing the exposure time to the detection mechanisms; and (2) postdetection delay enhances the probability of neutralization by providing increased time for security force reaction. The primary performance measures for this function are, of course, the penetration delay times attributable to each of the various delay-inducing elements such as terrain, fences, walls, doors, locks, guards, back-up security forces, etc. These delay times can be specified as expected values or in more detailed formats as probability distributions. They also apply across the spectrum of weapon status.

### 3.2.6 Neutralization

The neutralization function refers to the actions taken by the security system in countering an adversary action. The results of neutralization signify the level of success of the security system in preventing or minimizing a nuclear accident or significant event. The neutralization function does not necessarily imply the use of force or even the initiation of other active measures. For example, the mere existence of passive barriers may cause sufficient difficulties to an intruder to cause him to abandon his attempted penetration. For weapons in stationary status (i.e., in temporary or long-term storage) or in transit by ground vehicles, security system performance is related to one or both of the following two factors: depth of adversary penetration, and the ultimate status of the defended weapons. Depth of adversary penetration can be specified either as a continuous distance function or as a discrete set of points that signify critical plateaus along an adversary's action path. The ultimate status of the defended weapons depends on whether the weapons are destroyed, damaged, or removed, or remain undisturbed. In addition, the status can include compromise of classified weapon and security system information. The associated candidate performance measures then are as follows: <u>the cumulative probability of adversary penetration as a function of depth of penetration</u>; <u>the probability that a weapon is destroyed</u>; <u>the probability that a weapon is damaged</u>; <u>the probability that a weapon is stolen</u>; and <u>the probability that classified information is obtained</u>. These performance measures do not cover one additional facet of security system performance--that of employing excessive force against inadvertent or peaceful intruders. Hence, an additional performance measure to be considered is <u>the probability of using excess force against inadvertent or peaceful intruders</u>.

For weapons that are under airborne movement the performance measures related to the ultimate weapon status still apply, but those related to depth of adversary penetration do not. These latter are replaced by measures related to the success of the aircraft transporting the nuclear weapons in avoiding destruction, either through escape or a successful forced landing. Hence, for air transit cases, performance measures in lieu of penetration denial include <u>the probability that the aircraft transporting the weapons survives to its destination</u>, and <u>the probability that the aircraft does not reach its destination but does make a successful forced landing</u>. It should be noted that as soon as the aircraft lands, the weapons aboard are considered to revert to a temporary storage status, and the appropriate performance measures for this status would then be applicable for any ensuing adversary actions.

# SECTION 4

# SIMULATION/TESTING INTERFACE

## 4.1 General

Computer simulations, if properly designed and applied, can be extremely valuable tools to be used in support of test programs directed to evaluating the effectiveness of TNF security systems under operational conditions. The constraints of both time and cost impose severe limitations on the amount and scope of testing that can be conducted. Furthermore, certain facets of security system operations are untestable due to safety considerations. With proper planning, simulations can expand the scope and depth of the evaluation process in addition to providing valuable insights for use in test planning. Testing, on the other hand, can enhance the credibility of simulation outputs by providing near-real-life results that can be used for simulation validation and/or calibration. Thus, simulation and testing can interact synergistically with one another to provide for a broad-based, efficient evaluation program.

The interface between simulation and testing can take many forms, depending on the level of testing, the simulation credibility and complexity, and attitudes of the test planners and analysts toward simulations, and many other factors. In the next subsection, a representative interface is presented that attempts to cover most of the useful interactions between simulation and testing.

## 4.2 Representative Interface

A representative interface between simulation and testing is illustrated in Figure 4.1. For this case, it is assumed that the security system*

*System, as used here, could encompass the total security system or may refer only to a major subsystem sufficiently configured to perform at least one of the primary security system functions (dissuasion, detection, assessment, communication, delay, and neutralization).

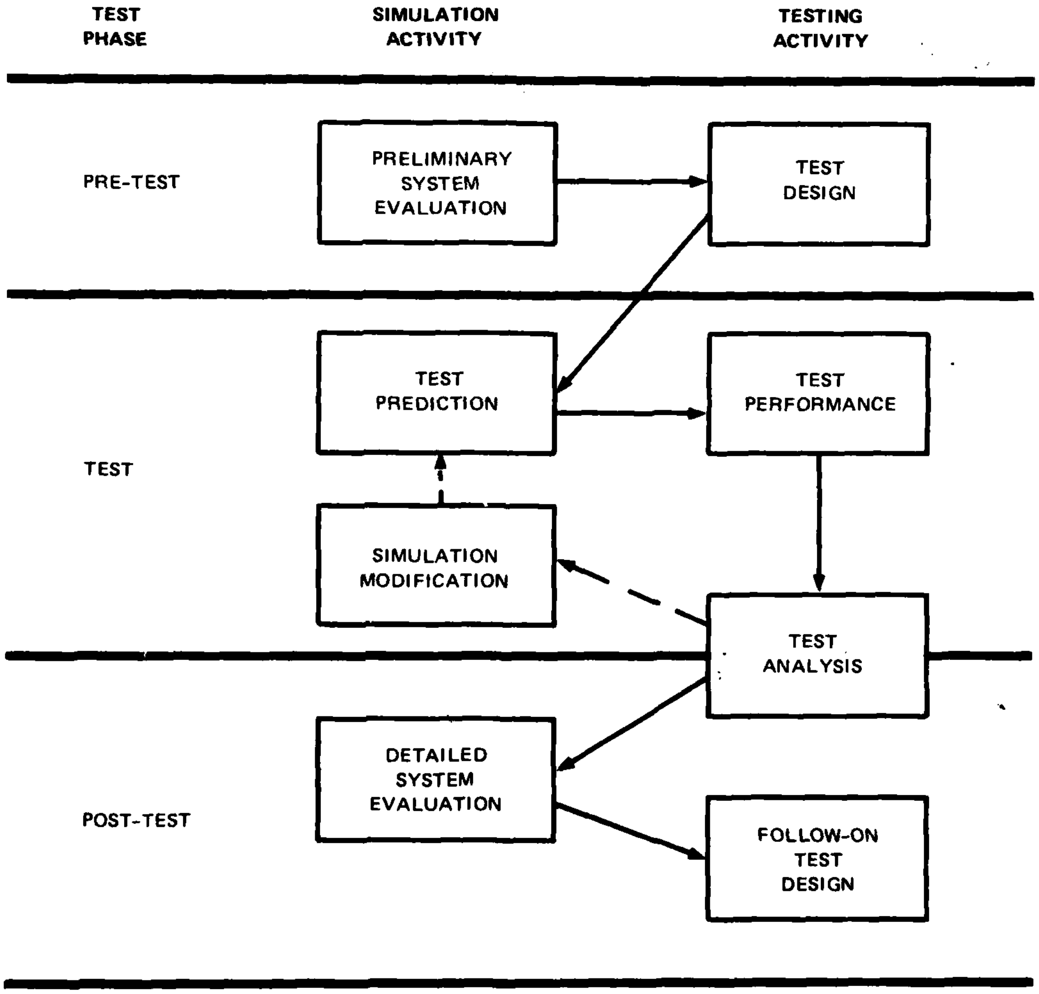


FIGURE 4-1 SIMULATION/TESTING INTERFACE

(equipment, personnel, and procedures) is either in existence or at least adequately designed to be configured for system testing.

### 4.2.1 Pre-Test Phase

During the pre-test phase of a test program, simulations can play an important role in the test planning process. Because testing can be an expensive and time-consuming process, the test planners must be judicious in their establishment of the test design. By using simulations to conduct a preliminary system evaluation, including sensitivity analyses, valuable insights can be gained with regard to many of the test design elements. Such an evaluation can examine the sensitivity of system performance to numerous variations in natural and man-made environmental factors, providing a basis for test site selection, location of test instrumentation, and the specification of critical environmental factors to be varied during the test. The preliminary system evaluation can also assist in the establishment of the level of test required. Undeı some environmental conditions, the results of the evaluation may indicate that only specific subsystems need be subjected to test, while under other environmental conditions the results may indicate the requirement for a full system test. The simulation results can also provide indications as to upper and lower bounds for the various test elements requirements, such as number of intrusion detection devices, barriers, guard forces, and so on. The above are but examples of the numerous ways a preliminary system evaluation using simulations can provide assistance in establishing an efficient test design within budget and time constraints.

In establishing the test design, the test planners may want to include some cases directed primarily to the enhancement of the validity of the simulations. It may be that some results obtained during the preliminary system evaluation will appear contrary to expectations. Selected cases may then be included in the test design to either verify or disprove the simulation results. Another area where testing can enhance simulation validity is in the establishment of a sound input data base.

Although sensitivity analysis is one means of circumventing suspect data inputs, this can become very time consuming and expensive so that data input verification through testing can prove fruitful in the long run.

Although the flowchart of Figure 3.1 indicates a one-way flow from preliminary system evaluation to test design, the procedure may well be iterative in nature. That is, after an initial evaluation, the test planners, in the course of designing the test, may well desire that some additional simulation runs be conducted in order to fine-tune some test design elements.

### 4.2.2 Test Phase

Once the test design has been finalized, the process moves into the test phase. Simulations can again provide useful assistance in supporting the tests. Initially, the simulations can be exercised to provide predictions of the expected test results. This provides a standard of comparison for the test analysts to monitor during the performance of the testing. If the results of the tests, as they continue to build up, conform within practical bounds to the predicted results, then everything is in accord, thus providing an enhancement to the credibility of the simulations and the tests. If, on the other hand, unexpected test results occur, then analysis should be conducted to determine the casue of the discrepancies. This analysis, which could make use of the simulations, may uncover an error in the test performance such as non-adherence to test design parameters, faulty instrumentation, or improper test procedures. After corrective action is made, the testing then continues. If such is not the case, the the onus is on the simulations themselves. Analysis should then be conducted to determine the nature of the simulation errors and to establish suitable simulation modifications to correct the deficiencies. Once accomplished, the simulations are again exercised to predict the expected test results and thus establish a new standard for comparison to be used as the testing continues.

### 4.2.3 Post-Test Phase

After the testing has been completed, a detailed analysis of the test results is conducted. The results of this detailed analysis will either corroborate the simulation predictions, and hence build confidence in the use of the simulations, or will uncover discrepancies in the simulations. If the discrepancies are small, then minor corrective modifications can be made, resulting in a finer calibration of the simulations. If the discrepancies are large, then major simulation modification or redesign will be required. Once the simulations are brought into harmony with the test results, then the simulations can be used to conduct a detailed system evaluation. This detailed evaluation will be useful in filling gaps not covered in the testing phase and also in indicating the bounds within which the test results are applicable. This evaluation may also uncover problem areas not considered during the test program and hence provide the basis and insights for establishing follow-on test designs. This would lead to another cycle through the simulation/testing interface.

## 4.3 Simulation Characteristics

There are several important characteristics that simulations should possess in order to be of useful assistance in the conduct of a testing program. These are discussed in the following subsections.

### 4.3.1 Completeness

Since a testing program for TNF security systems could conceivably cover every aspect of security system operations, the simulations themselves must also be capable of covering all aspects of these operations. When certain aspects are not testable due to safety considerations, then it is all the more important that simulations address these aspects. Although one large, complex simulation could be designed to achieve this goal, it is more than likely that a set of simulations would prove more efficient in the long run, especially since the nature of security system operations significantly differs under fixed site, ground movement, or air movement scenarios. The main concern is that the simulations adequately cover the broad range of possible confrontation situations and address each of the measurable security system functions (dissuasion, detection, assessment, communication, delay, and neutralization).

### 4.3.2 Dual Complexity

One desirable, though not necessary characteristic that enhances the usefulness of simulations for testing support is a dual complexity capability. This refers to the availability of simulations of two different levels of complexity: a set of relatively aggregated simulations, and a set of fairly detailed simulations. The aggregated simulations are useful for obtaining rough estimates of system effectiveness over a wide range of input variations and identifying critical areas for deeper analysis. The detailed simulations are then useful for fine-grained analysis for a much narrower band of input sets. For use in a testing program, the set of detailed simulations are a necessity, while the set of aggregated simulations are desirable but not required.

### 4.3.3 Modularity

The requirement for modularity has become an almost universal criterion in the development of detailed simulations. The ever-present demand for change and improvement mandates that distinct functions be isolated, when possible, in separate programming modules. Individual modules can then be modified or replaced without upsetting the remainder of the program. In light of the dual complexity characteristic discussed in the previous subsection, modularity becomes an even more desirable characteristic. Interchangeability of aggregated and detailed modules of like functions allows the user to analyze in detail changes that affect only specific system functions, while maintaining a gross analysis capability for the other system functions.

### 4.3.4 Test Compatibility

Another required characteristic of simulations in support of test programs is that they be compatible with the test parameters. Simulation input requirements should include a mirror image of test input variables or, at the worst, be accurately derivable from them. The simulation outputs must also be compatible with outputs obtained from testing or at least be suitably transformable for comparison purposes.

### 4.3.5 Machine Independence

The usefulness of simulations in support of test programs is enhanced if they are programmed in a universal language, such as FORTRAN, and are not burdened with any machine-dependent operations, such as word packing. For large test programs that may involve geographically widely dispersed test sites, machine independence virtually becomes a requirement. Utilization of computer facilities at or near the test site generally enhances the use of simulations as supporting tools, especially during the test phase where timely support is required. Although long-distance Telex systems are improving, transmission problems still arise and time zone variations can limit the usable periods for coordinated simulation and test exercises.

### 4.3.6 Usability

Although an implicit requirement, the characteristic of usability should be mentioned for emphasis. Usability here refers to the requirement that the simulations be capable of near-real-time support during the test phase. Long data preparation and program running times degrade the usefulness of simulations in support of test operations.

Complex operating instructions and hidden program anomalies can cause havoc unless the user is highly conversant with the program. Thorough and clear documentation is a requirement for extended and multiple usage of simulations. In situations where personnel turnover could be a problem, training manuals should be made available. Simulation modifications should also be well documented.

# SECTION 5

# AVAILABILITY OF SIMULATION TOOLS

## 5.1 Literature Search

A computer search of the National Technical Information Service (NTIS) Library using the DIALOG system was conducted to identify simulations that might be applicable for use in support of the $TNFS^2$ Program. This library search was augmented by a manual search of the Defense Documentation Service (DDC) Abstracts, which includes limited distribution and classified reports not contained in the NTIS Library. Over 1,100 abstracts were identified in these two literature searches. An initial screening of these abstracts resulted in identifying approximately 110 reports that might be relevant to the purposes of this study. Several of these reports were already available at SRI and the remainder were ordered through the appropriate documentation service. Additional reports that might be applicable were identified subsequent to the literature searches, and several of these were obtained and included in the simulation review. This resulted in a total of 129 reports* that were reviewed in this analysis. The reports were segregated into the following categories, with the number included in each category indicated by parenthesis:

- Simulations (93)
- Simulation catalogs and comparisons (12)
- Equipment, concepts, and input data (12)
- Study plans and progress reports (12).

An initial screening of 93 simulation reports was conducted to determine those that might be directly applicable to security system evaluation. A total of 41 simulations were identified as possible candidates,

*These are listed as References 25 to 153 at the end of this report.

and these were subjected to more detailed analysis. Table 5.1 identifies these simulations and indicates their possible applicability to the evaluation of security system functions. The detailed analyses used as guidelines the set of desirable simulation characteristics discussed in Section 4.3 of this report: completeness, dual complexity, modularity, test compatibility, machine independence, and usability. These detailed analyses identified 10 simulations that sufficiently address the security system evaluation problem to warrant further consideration as candidates for simulation tools in support of the TNFS$^2$ Program. The first 10 entries of Table 5.1 identify the selected simulations. Their applicability as support tools to the TNFS$^2$ Program are discussed in subsequent subsections.

The primary reason for rejecting many of the other simulations analyzed was that they did not directly address the security system evaluation problem. Several are two-sided simulations of infantry combat (some with supporting air fire) that are not readily amenable to modifications that would be required in either the fixed-site or ground-movement scenarios for security system evaluations. Others are either one-on-one simulations for evaluating air defense weapon effectiveness against fixed and rotary wing aircraft, or are simulations for evaluating the effectiveness of attack helicopters in support of ground combat operations. Secondary reasons for rejection were non-usability (extensive data input preparation or long running times), obsolescence, and inferior implementation.

The next three subsections segregate the selected simulations into three classes (fixed site, ground transport, and air transport) and present a discussion of their applicability as supporting tools to the TNFS$^2$ Program.

## 5.2 Fixed-Site Simulations

### 5.2.1 Simulation Summaries

There we:e four simulations identified that could be applicable as tools in support of the TNFS$^2$ Program relative to the security of weapons located at fixed sites (permanent or temporary). Summary

Table 5.1

SIMULATION APPLICABILITY

| No. | Simulation* | Developing Agency | Reference No. | Fixed Site | | | | | | Grou | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Dissuasion | Detection | Assessment | Communications | Delay | Neutralization | Dissuasion | Detecti |
| 1. | Armed Escort Model | Electronic Associates, Inc. | 25,26 | | | | | | | | |
| 2. | EASI | Sandia Laboratories | 27-30 | | X | X | X | X | | | |
| 3. | FESEM | Sandia Laboratories | 31-33 | X | X | X | X | X | X | | |
| 4. | Pathfinding Codes | Sandia Laboratories | 34-39 | | X | | | X | | | |
| 5. | PENAIR | Naval Postgraduate School | 40 | | | | | | | | |
| 6. | SABRES | Sandia Laboratories | 41-43 | | | | | | | | |
| 7. | Schaffer's Ambush Model | Naval Postgraduate School | 44 | | | | | | | | |
| 8. | SOURCE | Sandia Laboratories | 42,43,45 | | | | | | | | X |
| 9. | TSEM | The BDM Corporation | 46-48 | | | | | | | X | X |
| 10. | VISA | Science Applications, Inc. | 49,50 | X | X | X | X | X | X | | |
| 11. | Adversary Action Modeling | Lawrence Livermore Lab. | 51-53 | | X | X | | | | | |
| 12. | AIDM Suppression Model | BDM Services Co. | 54 | | | | | | | | |
| 13. | AIRCAV | Vector Research, Inc. | 55,56 | | | | | X | X | | |
| 14. | AMSWAG | AMSAA | 57 | | | | X | X | X | | |
| 15. | Analytic Engagement Model | Sandia Laboratories | 58 | | | | | X | X | | |
| 16. | ARMREC | Naval Postgraduate School | 59 | | | | | | | | |
| 17. | Bonder/IUA | AMSAA | 60 | | | | | X | X | | |
| 18. | Breakpoints in Land Combat | Naval Postgraduate School | 61 | | | | | X | X | | |
| 19. | Brookhaven PPM | Brookhaven National Lab. | 62 | | X | X | X | X | | | |
| 20. | CARMONETTE | General Research Corp. | 60,63-71 | | | | X | X | X | | X |
| 21. | Countermeasures Engagement Analysis | Air Force Inst. of Tech. | 72 | | | | | | | | |
| 22. | Daylight Assault Model | Naval Postgraduate School | 73 | | | | | X | X | | |
| 23. | DYNTACS | Ohio State University | 60,74-80 | | | | X | X | X | | X |
| 24. | EVADE | AMSAA | 81 | | | | | | | | |
| 25. | FAST-VAL | Rand Corporation | 82-85 | | | | | X | X | | |

*A brief description of each of these simulations is provided in the Appendix.

1

| Fixed Site | | | | | | Ground Transport | | | | | | Air Transport | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Dissuasion | Detection | Assessment | Communications | Delay | Neutralization | Dissuasion | Detection | Assessment | Communications | Delay | Neutralization | Dissuasion | Detection | Assessment | Communications | Delay | Neutralization | Comments |
| | | | | | | | | | | | | | X | | | X | X | Some direct application. See Section 5.4.1.2. |
| | X | X | X | X | | | | | | | | | | | | | | Some direct application. See Section 5.2.1.2. |
| X | X | X | X | X | X | | | | | | | | | | | | | Some direct application. See Section 5.2.1.3. |
| | X | | | X | | | | | | | | | | | | | | Some direct application. See Section 5.2.1.1. |
| | | | | | | | | | | | | | X | | | X | X | Some direct application. See Section 5.4.1.1. |
| | | | | | | | | | | X | X | | | | | | | Some direct application. See Section 5.3.1.3. |
| | | | | | | | | | | X | X | | | | | | | Some direct application. See Section 5.3.1.1. |
| | | | | | | | X | X | X | X | | | | | | | | Some direct application. See Section 5.3.1.2. |
| | | | | | | X | X | X | X | X | X | | | | | | | Some direct application. See Section 5.3.1.4. |
| X | X | X | X | X | X | | | | | | | | | | | | | Some direct application. See Section 5.2.1.4. |
| | X | X | | | | | | | | | | | | | | | | Only addresses insider theft of small amounts of special nuclear material. |
| | | | | | | | | | | X | X | | | | | | | Only addresses simulation of suppression. |
| | | | | X | X | | | | | X | X | | | | | | | Two-sided infantry combat simulation with supporting air fire. |
| | | | X | X | X | | | | X | X | X | | | | | | | Two-sided infantry combat simulation--inordinate amount of input. |
| | | | | X | X | | | | | | | | | | | | | Number of adversaries and guards extremely limited. |
| | | | | | | | | | | | | | X | | | X | X | Armed reconnaissance attack helicopter simulation. |
| | | | | X | X | | | | | X | X | | | | | | | Two-sided armored infantry combat simulation. |
| | | | | X | X | | | | | X | X | | | | | | | Aggregated simulation relying on much subjective judgment. |
| | X | X | X | X | | | | | | | | | | | | | | Completely deterministic and oversimplified. |
| | | | X | X | X | | X | | X | X | X | | | | | | | Complex two-sided armored infantry combat simulation. Highly machine dependent. |
| | | | | | | | | | | | | | X | | | X | X | Incomplete one-on-one air vs. ground simulation. |
| | | | | X | X | | | | | X | X | | | | | | | Old Lanchester-type two-sided infantry combat model. |
| | | | X | X | X | | X | | X | X | X | | | | | | | Complex two-sided armored infantry combat simulation. Machine dependent. |
| | | | | | | | | | | | | | X | | | X | X | Attack helicoptor simulation. |
| | | | | X | X | | | | | X | X | | | | | | | Large-scale armored infantry combat simulation. |

| No. | Simulation* | Developing Agency | Reference No. | Fixed Site | | | | | | Ground Tr | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Dissuasion | Detection | Assessment | Communications | Delay | Neutralization | Dissuasion | Detection | Assessment |
| 26. | FIREFIGHT | SRI International | 86 | | | | | X | X | | | |
| 27. | GCC Firefight | Naval Weapons Lab. | 87 | | | | | X | X | | X | |
| 28. | Helicopter vs. Tank Duel | Naval Postgraduate school | 88 | | | | | | | | | |
| 29. | ICM | Army Concepts Anal. Agency | 89 | | | | | X | X | | | |
| 30. | Interdiction Model | Rand Corporation | 90 | | X | | | X | X | | | |
| 31. | ISEM | Sandia Laboratories | 91-94 | X | X | X | X | X | X | | | |
| 32. | IUA | CACDA | 60,95,96 | | | | | | | | X | |
| 33. | JOLIWACO | Control Data Corporation | 97,98 | | | | | | | | | |
| 34. | Markov Engagement | Vector Research, Inc. | 99 | | | | | X | X | | | |
| 35. | Math Model of Infantry Combat | Naval Postgraduate School | 100 | | | | | X | X | | | |
| 36. | Penetration Attrition Model | Inst. for Defense Analysis | 101 | | X | | | X | X | | | |
| 37. | SDC Transportation Model | Systems Development Corp. | 102,103 | | | | | | | | | |
| 38. | SIAF | TRW Systems Group | 62,<br>104-110 | | | | X | X | X | | X | |
| 39. | Supporting Fire Model | Naval Postgraduate School | 111 | | | | | | | | | |
| 40. | TAM | Army Concepts Anal. Agency | 112 | | | | | | | | X | X |
| 41. | TRW PPM | TRW Systems Group | 62 | | X | X | X | X | | | | |

1

Table 5.1 (Concluded)

| te |  | Ground Transport |  |  |  |  |  | Air Transport |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Delay | Neutralization | Dissuasion | Detection | Assessment | Communications | Delay | Neutralization | Dissuasion | Detection | Assessment | Communications | Delay | Neutralization | Comments |
| X | X |  |  |  |  | X | X |  |  |  |  |  |  | Limited expected value simulation of small unit engagements. |
| X | X |  | X |  |  | X | X |  |  |  |  |  |  | Large-scale armored infantry combat simulation. Obsolete programming language. |
|  |  |  |  |  |  |  |  |  | X |  |  | X | X | One-on-one helicopter vs. tank simulation. Program has errors. |
| X | X |  |  |  |  | X | X |  |  |  |  |  |  | Infantry combat simulation. Heavy emphasis on ammunition expenditures. |
| X | X |  |  |  |  |  |  |  |  |  |  |  |  | Game-theory optimization simulation. Not an evaluation tool. |
| X | X |  |  |  |  |  |  |  |  |  |  |  |  | Mainly concerns insider theft of small amounts of special nuclear material. |
|  |  |  | X |  |  | X | X |  |  |  |  |  |  | Complex tank-anti-tank simulation. |
|  |  |  |  |  |  | X | X |  |  |  |  |  |  | Large-scale insurgency--counterinsurgency man/machine war game. |
| X | X |  |  |  |  | X | X |  |  |  |  |  |  | Initial concept formulization of a limited-engagement simulation. |
| X | X |  |  |  |  | X | X |  |  |  |  |  |  | Limited Lanchester-type infantry combat simulation. |
| X | X |  |  |  |  |  |  |  |  |  |  |  |  | Stochastic simulation of series of one person infiltration attempts. |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  | Not a simulation. |
| X | X |  | X |  | X | X | X |  |  |  |  |  |  | Complex small unit combat simulation. Large amount of input. Subroutines useful. |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  | Aggregated artillery supporting-fire allocation simulation. |
|  |  |  | X | X |  |  |  |  |  |  |  |  |  | Large-scale target acquisition simulation. |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  | Fixed-site simulation. No neutralization. Documentation not provided. |

2

descriptions of these simulations are presented in the following subsections. These summaries indicate the type of simulation, the nature of the input data, the security system functions addressed, and the nature of the output data.

### 5.2.1.1 Pathfinding Codes

The Pathfinding Codes discussed here represent a set of computer codes developed by Sandia Laboratories to establish optimum paths for adversaries to follow in covert sabotage, control, or theft attempts against fixed nuclear sites. The sites are defined by a graph of nodes and connecting arcs. Each node and connecting arc is provided a weight factor. The weight factor can be the expected adversary traversal time through a node or over an arc; it can be the probability of detection while traversing through a node over an arc; or it can be both. Given a starting node, the adversary is to proceed along arcs and through nodes to a goal node (the location of nuclear material). In the theft case, the adversary must also proceed back and exit at the starting node. The computer codes are designed to determine the optimum path for the adversary, where in one case the optimization is in terms of minimizing the adversaries' time to reach his goal (and escape, in the theft case) and in another case the objective is to minimize the probability of detection. A combined case considers a locus of nodes that are no more than a security force's response time away from the goal node. The algorithm then selects the optimum path by minimizing the detection probability into this locus of nodes and then minimizing the traversal time to the goal node. The algorithm used consists either of a "back-track" method or a modification of Dijkstra's algorithm. One code not only gives the "shortest" path, but the "K-shortest"* paths. The documentation is clear and complete, and the code listings are provided. These codes represent aggregated simulations that touch on the detection and delay functions of a security system. Consideration of the security force response times adds a gross treatment of the combined assessment/communication function.

*The first K paths ranked by increasing length of time to accomplish mission.

### 5.2.1.2 EASI

The Estimate of Adversary Sequence Interruption (EASI) simulation is an aggregated, analytic simulation developed by Sandia Laboratories that provides an estimate of the security system's capability to interrupt an adversary's attempt to sabotage or steal nuclear material at a fixed nuclear site, where interruption refers to a response force arriving at the adversary's terminal point [location of nuclear material (weapons) for sabotage, and site exit point for theft] prior to the adversary's arrival there.

The inputs to the simulation include the number of "tasks" that the adversary must perform along a preanalyzed physical path to his objective and subsequent exit (for theft only). The "tasks" include getting by intrusion detection devices, crossing open areas (possibly under surveillance), overcoming barriers, and sabotaging or stealing the nuclear material (weapons). For each "task," inputs include the probability of detection and the parameters of the distribution of task performance times (mean and standard deviation of an assumed normal distribution). Additional inputs include the security system's probability of successful communication given a detection and the parameters of the response force's response time distribution (assumed as a normal distribution).

For each task, beginning with the last, the program determines the probability of interruption given that detection occurred during the performance of that task. These results are then probabilistically combined, considering both detection and communication probabilities, to determine the overall probability of interruption, which is the program's only output. The program in performing the above computations makes use of the logistic approximation to the normal distribution.

The program is simple enough to run on a hand-held programmable calculator. The program can also be run on a timesharing or batch system and has a computer graphics package that provides two- and three-dimensional plots of the probability of interruption as a function of one or two input variables, respectively. As indicated above, the program is an aggregated simulation that addresses the detection, assessment (included in the detection probability input), communication, and delay functions of a security system. It does not, however, address the neutralization function. The program is well documented, and includes a user manual with program listings provided.

#### 5.2.1.3 FESEM

The Forcible Entry Safeguards Effectiveness Model (FESEM) is a combined time-stepped, event-sequenced Monte Carlo simulation designed to evaluate the effectiveness of a security system against covert attempts by an adversary force to sabotage or steal nuclear material (weapons) from a fixed nuclear site.

The inputs to the simulation are quite varied. The site attribute inputs include the number of barriers (maximum of 15), the numbers of on-site and off-site response forces (maximum of 5 each), a guard dedication indicator (low, medium, high), the barrier number at which air attacks commence, surveillance detection probability for air attacks, air surveillance alarm time distribution,* landing time distribution, the number of the barrier at which patrol surveillance begins, the patrol surveillance alarm time distribution, the muster force size (minimum number of guards required to initiate an engagement during adversary ingress), and the distributions denoting the adversary's speed (one for on-foot movement and one for in-vehicle movement). A barrier as used in this simulation is any node or path segment where there is an associated intrusion detection device or delay mechanism or both. The barrier inputs, specified for each barrier, include the distance to the next barrier, the barrier delay distributions [depending on whether adversary is on foot or in vehicles, and whether the adversary is with high explosives (HE) or without], probabilities of alarm for external and internal-assisted attacks, the assessment delay distribution, an indicator of

*All operational distributions are assumed triangular, with the parameters specified as input being the minimum, mode, and maximum values of the distribution.

whether HE is used on this barrier, the probability of HE detection if used, the distribution for the HE set-up and detonate time, and number of the barrier that is activated (if any) if the present barrier trips an alarm, and distribution for the activate delay time, if applicable. Also included are the theft completion time distribution, two sabotage completion distributions (one for less than eight individuals and one of eight or more individuals), and a building-exit delay distribution for thief-guard encounters. Response force inputs, specified for each response force, include the number of guards in the response force, the communication probabilities for external and internal-assistec attacks, the on-site and off-site force alert delay-time distributions, and the response-time distributions. The adversary attributes include the number of attackers, weapon type (small arms versus automatic weapons), resources for barrier penetration (tools without HE versus tools with HE), mobility of attacker (on foot, land vehicles, or air vehicles), dedication and sophistication of attackers (low, medium, high), and type of attack (sabotage/internal assistance, sabotage/external, theft/internal assistance, or theft/external). The simulation has the capability to randomly select each of the attacker attributes, assuming uniform distributions over ranges for each attribute that are specified by input. If the upper and lower bounds on the range for a specific attribute are equal, then that attribute is fixed for a given run.

The simulation begins by randomly selecting a set of adversary attributes within the bounds specified by the input (it is possible to hold this first set of attributes fixed for subsequent attacks evaluated during the remainder of the run, if so desired). At time zero, the adversaries have either arrived at the first barrier (on foot or in vehicles) or the adversaries' aircraft begins to land in the vicinity of the input specified barrier, at which time air attacks commence. In the latter case, a determination* is made if the aircraft was detected and, if it was, the time at which an air surveillance alarm is sounded. Also,

*All events and event times are determined by Monte Carlo methods, except for adversary-guard engagements.

the time at which the landing is completed (the adversaries arrive on foot at the specified barrier) is established. Event occurrence times are stored in chronological order and processed in time sequence. Arrival at a barrier induces a subsequent break barrier event and possibly a detection event, which in turn induces an alarm event and possibly a barrier activate event. If HE is used to break through a barrier, the HE set-up and detonate time is determined. If the HE is detected, then an HE alarm event is scheduled. A break barrier event induces a subsequent barrier arrival event. An alarm event induces a communication event and, if successful, the latter induces an alert event, which in turn induces a response force arrival event. A patrol surveillance alarm event is generated when the adversaries reach the outermost barrier that is included in the patrol region. If a response force arrival event occurs before the adversaries have reached their objective, then an engagement is initiated if the response force equals or exceeds the muster force requirement. Once the adversaries reach their objective, then the muster force requirement is no longer valid. Engagements between adversaries and guards are evaluated through use of a time-stepped numerical integration of a 10th-order nonlinear differential equation with time-varying coefficients. When outnumbered, the defenders use delay and sniper tactics, and will assault when strength allows. The engagement lasts until attrition is such that preestablished survivor limits are obtained. The applicable survivor limits are dependent on the dedication levels of the adversaries and of the guards. If the guards win the engagement, then the attack is over with a security system win. If the adversaries win, then they continue along their action path and may be challenged by later-arriving response forces. If the adversaries complete the sabotage of the nuclear material (weapons) or exit the site boundary following theft, then the attack is terminated with an adversary win. A computer run consists of a large number of independent attacks.

The FESEM output options are quite varied and are controllable by the user. A collected statistics report is available that provides a number of outcome statistics for several variables. The collected statistics are the mean, standard deviation, standard deviation of the mean, coefficient of variance,* minimum value, maximum value, and total number of observations during a computer run. The observations are divided into two categories, sabotage success, and theft success. The variables considered are the adversary attributes (number of attackers, dedication level, etc.), in addition to the start time for battles and the time for battles. Another report presented is the Summarized Results Output. This table presents the probability of losses and wins for sabotage and theft attacks as functions of attack force size, attack mobility, and type of attack. Overall probabilities of defender and attacker success are also summarized. Line-printer plots of the summary output are also available. In addition to these summary output reports, histograms on up to 15 variables may also be generated.

The simulation is a relatively detailed, Monte Carlo simulation that addresses all six security system functions.† The program is written in the FORTRAN-based GASP-IV simulation language. Excellent documentation is provided, including a user's manual and program listing.

#### 5.2.1.4 VISA

Vulnerability of Integrated Safeguards Analysis (VISA) is an evaluation method that can be used to evaluate the effectiveness of fixed-site security systems against hostile encounters, both overt and covert. The method is divided into three sections: preparation, analysis, and assessment. The preparation section is simply a formalization of the site data input preparation process, and the assessment section is essentially concerned with the storage of case analysis results, with procedures to assess these results at different levels of detail via an interactive display terminal. The analysis section includes the principal evaluation tools and is the subject of the remainder of this subsection.

*Coefficient of variance--the ratio of the standard deviation of a distribution to its arithmetic mean.

†As per the discussion on dissuasion in Section 3.2.1, it is assumed that the dissuasion function is addressed if all of the other five security system functions are addressed.

The analysis section consists of four analysis modules (Path, Detection, Containment, and Interruption) and requires two data bases (Detection Mechanism, and Delay Mechanism and Engagement). The beginning point is to define the case to be analyzed. A case consists of the threat (adversary goal, number of adversaries, and insider/outsider mix), the target (location, and amount of material for theft or equipment or fixture for sabotage), and the adversary action sequence (AAS), which is broken down into segments (entry and destruction for sabotage, and entry, acquisition, and removal for theft). The Path Analysis Module is actually a procedure for decomposing each AAS independent segment into independent paths (each path represents a set of adversary tasks or delay and detection devices encountered) and for possible initial ranking of applicable paths for use in subsequent analysis. This module is a combination of manual activities involved in identifying the path components through fault-tree analysis and automated procedures using boolean logic to combine path components and establish a path ranking according to a prespecified criterion (minimize detection probability for covert segments or minimize expected delays for overt segments). In VISA, a segment is treated both as overt and as covert. Later on in the procedure, segments are combined to determine covert-overt combination action sequences.

The Detection Analysis Module is used to calculate a figure of merit for the security system performance against covert adversary actions for all the established paths. The figure of merit used is the probability of detection, which includes assessment--that is, the probability that the system will initiate actions to interrupt the AAS. The calculation of the figures of merit is a straightforward procedure of combining detection probabilities based on the number of adversaries, their goal, the target, the segment, and the path. These path detection probabilities are computed for each path component (node) at which detection can occur, and then are stored for subsequent use in the Interruption Analysis Module. The required detection mechanism detection probabilities are obtained from the Detection Mechanism Data Base. This data base consists of detection probabilities for all such mechanisms for all initial conditions (facility operating state, mechanism operating state, adversary state of preparation) and all employee access classifications (outsiders, and insiders with authorized access to the facility, to areas within the facility, and to protective mechanism). The data are obtained from models of each individual mechanism or from experiments and tests. The data include both the vulnerabilities of the mechanisms to tampering and the detection probabilities under all appropriate conditions.

The Containment Analysis Module parallels the Detection Analysis Module, except that this module considers overt paths. The figures of merit generated by this module for each path and set of conditions are the containment probability--that is, the probability that the security system contains the target material (weapons) within the facility (site) after an AAS is detected to be in progress. Since detection can occur at a number of places along a path, the containment probabilities calculated (and stored for subsequent use) are conditioned on the path segment at which detection occurs. Thus, for each path segment at which a detection can occur (considering all of the covert adversary paths being analyzed), a containment analysis is conducted. The analysis is a two-step procedure. First, a simple analytical model is used to rank paths in accordance with some measure of containment probability. (An initial method considered time to complete mission as the ranking measure. Some subsequent effort was devoted to injecting a gross evaluation of containment into the measure used. This results in an intuitively better approach, but requires additional work.) From this path ranking, only the best paths (from an adversary's point of view) are selected for detailed analysis, the objective of which is to determine the worst-case path (from the security system point of view). For the detailed analysis, a network Monte Carlo simulation is used that includes aggregated delay time and engagement simulations. This network simulation is coded in the Q-GERT queueing network simulation language. For VISA, a nine-line network is used that allows for four adversary action lines (a main line and up to three covering lines), four guard force action lines (one assessing and three responding), and an off-site response force action line. Action lines correspond to possible paths the different groups can take, with the network layout describing branch points at decision (outcome) nodes. The adversaries proceed along the main action line until the detection segment is reached, at which time they may break up into a goal group and covering groups. After an assessment delay, the guard forces and response force are activated along their action lines. As each group proceeds along its action line, with Monte Carlo sampled delay times obtained from input distributions, encounters may occur between adversary and guard groups. These encounters initiate engagements that are evaluated by use of the engagement simulation. The engagement simulation is a simple Monte Carlo type that depicts individual fire by a guard or adversary (firer chosen randomly based on fraction of personnel on each side) with assessment as to whether or not a casualty occurred. Engagement continues until prespecified disengagement criteria are met. The inputs required are the distribution parameters for the efficiencies (casualty/shot) of the guards and adversaries for the specified type of engagement, time per shot, and disengagement criteria inputs (percent attrition for an engagement end, number of personnel on a side for an engagement end, and a win probability value that is used with an empirical equation that determines an engagement end). The output of the engagement simulation includes the engagement winner, the number of survivors on each side, and the elapsed time of the engagement. For an engagement node of an action line in the network, there are several branch lines that depict the continuation of the action line, where each branch represents a possible outcome of the engagement. At the conclusion of the engagement, the proper branch for each action line is selected and the surviving personnel in each action group proceed along the proper branch line. These branch lines allow for action line termination, continuation along the planned path or an alternate path, regrouping with another group, and so on. The network simulation terminates when the adversaries are defeated or when they achieve their objectives.

A normal network simulation run consists of about 100 Monte Carlo simulations. The outputs are summarized in a computer-generated summary statistic table. This table presents the probabilities of adversary and guard wins, and various statistics on the elapsed intrusion time (mean, standard deviation, standard deviation of the mean, coefficient of variance, minimum value, and maximum value). These intrusion time statistics, including the win probabilities, are given for four output classes: all cases, adversary wins only, on-site guard wins only, and off-site guard arrivals only. For the latter three outcome classes, the means and standard deviations for the number of guards and number of adversaries remaining are also tabulated. Computer-generated histograms are also available for the intrusion times for each of the four outcome classes.

The network simulation runs in their entirety provide the containment probabilities for the various segments of the selected "worst-case" AAS candidates. These probabilities, together with the detection probabilities established in the Detection Analysis Module, are the basic inputs that go into the Interruption Analysis Module. This module appropriately combines the detection and containment probabilities for a given AAS to determine the overall figure of merit for that AAS, where this figure of merit is the probability that the security system prevents an adversary from achieving his objective. The figures of merit for each candidate AAS are then compared, and the AAS that exhibits the minimum value of this figure of merit is the "worst-case" AAS. This selected figure-of-merit value then represents a measure of effectiveness of the security system against the specified adversary threat.

The VISA method is a composite set of manual, analytical, and simulation procedures to be used in determining the effectiveness of a fixed-site security system against overt and covert actions of theft and sabotage. This set of procedures addresses all six of the security system functions. The main simulation included in this set of procedures is the network simulation used in the Containment Analysis Module. This simulation is written in the Q-GERT network simulation language. The documentation of the VISA method provides an overview of the various procedures, but is fairly difficult to follow. No computer listings are provided and the description of the network simulation model requires some knowledge of the Q-GERT methodology for a good understanding of the simulation structure and operations.

### 5.2.2 Discussion

The simulations summarized in Section 5.2.1 above are representative of the state of the art of fixed-site security-system simulation modeling. Although these are lacking in certain respects, it should be noted that effort is proposed or in progress to improve and expand these simulations. For example, Vector Research, Inc. is providing support to Sandia Laboratories in several areas involving combat simulations. One area is the development of a fixed-site neutralization simulation (Ref. 152), which may replace, or possibly complement, the neutralization subroutine used in the FESEM simulation. Science Applications, Inc. has also proposed some modifications and expansions to the VISA simulation, although funding has not as yet been received to go ahead with this work. Thus, it should be recognized that the simulations, though presently operational, are still in the development stage and some of their shortcomings will be addressed in the near future.

This discussion will now consider the six simulation characteristics identified in Section 4.3--that is, completeness, dual complexity, modularity, test compatibility, machine independence, and usability.

#### 5.2.2.1 Completeness

Completeness covers two areas: confrontations addressed, and security system functions modeled. The Sandia Laboratories set of simulations (pathfinding Codes, EASI, FESEM) are primarily directed toward initially covert actions by a small group of adversaries, with or without insider assistance. The adversaries are restricted to a single group traversing a preplanned path, with no allowance for altering the route when they become aware of being detected or are apprehended by guard forces. This set of simulations, then, does not directly allow for any diversionary activity, although the input values for response times could be altered to indirectly include the effects of such actions. The restriction to a single adversary action path also precludes consideration of most initially overt actions, where adversaries would most likely use diversionary and/or covering tactics. The VISA approach, on the other hand, does allow up to four action paths for the adversaries in the Containment Analysis Module's network simulation. This allows consideration of up to four separate adversary groups and thus provides a capability to consider diversionary and covering tactics for both initial covert and initial overt actions. This network approach also allows for prespecified contingency paths to be followed in the face of defender actions. Thus, the VISA methodology addresses a broader scope of confrontation situations than does Sandia's set of simulations.

Both the FESEM simulation and the VISA methodology address all of the defined security system functions. The more aggregated EASI simulation does not address the neutralization function.

5.2.2.2 Dual Complexity

Both the Sandia set of simulations and the VISA methodology include some consideration of a dual complexity approach. The EASI/FESEM combination represents an aggregated analytic approach (EASI) backed up with a more detailed Monte Carlo approach (FESEM), although the EASI simulation does not address the neutralization function. In the Containment Analysis Module of the VISA methodology, some effort has been included for developing an aggregated analytic approach to ranking alternative paths and then using the more detailed network simulation to analyze a subset of these paths that would appear more desirable from the adversary's viewpoint. However, the aggregated approach previously used does not adequately address neutralization, and expansions have been recommended, but not formalized.

5.2.2.3 Modularity

Of the Sandia simulations, both the EASI and FESEM simulations are modular in nature. Because of their analytic nature the Pathfinding Codes do not lend themselves to modular construction by security system function. In EASI, the two directly simulated functions (combined detection/assessment/communications and delay) are relegated to separate subroutines. In FESEM, approximately 22 subroutines are used to generate events, analyze engagements, and perform other required operations. In terms of the security system functions, these subroutines can be grouped together in subsets that address a specific function, with only a little relatively insignificant overlap across functions. The VISA methodology, by design, is also a modular approach with its four existing analysis modules. Furthermore, the network simulation, used in the Containment Analysis Module, is by nature also a modular type simulation.

### 5.2.2.4 Test Compatibility

The spectrum of inputs required by either the Sandia simulations or the VISA methodology is sufficiently broad to provide acceptable compatibility with the TNFS$^2$ Program requirements. The actual inputs to the simulations themselves will, in many cases, have to be derived from test input parameters. The VISA methodology includes several methods for performing such data transformations. On the output side, the VISA approach of segregating analysis modules provides a convenient structure for comparing simulation results with test results on a security system function level. FESEM, on the other hand, would require some modifications (not extensive) to provide additional accumulation and printing out of function-related outputs. The Pathfinding Codes and EASI simulation are essentially pre-test tools and are not designed (nor intended) to be compatible with testing activities.

### 5.2.2.5 Machine Independence

Both the Pathfinding Codes and the EASI simulation are programmed in the FORTRAN language. As such, both should be easily transferable to any computer system having a FORTRAN compiler. The FESEM simulation makes use of the FORTRAN-based GASP-IV simulation language, while the VISA network simulation makes use of the FORTRAN-based Q-GERT network simulation language. Each of these special-purpose languages is available in packages that are supposed to be easily adaptable to any up-to-date FORTRAN based system. Nevertheless, some bugs may be expected in the initial implementation of either of these specialized languages, although the extent of this problem is difficult to predict.

Other than the use of these specialized simulation languages, none of the simulations appear to be machine-dependent.

#### 5.2.2.6 Usability

All of the simulations summarized in this section require the establishment of a data base. However, once this data base is established, none of the Sandia simulations appear to present any difficulties in setting up cases and running the programs. The Sandia documentation is very detailed and easy to follow. The VISA methodology should not provide any great problems either, although it appears from the documentation that use of the network simulation will require some training relative to the Q-GERT network simulation language. Use of VISA will certainly require additional documentation with a good users manual as a minimum requirement. From the descriptions of all of the simulations, running time does not appear to be a problem for near-real-time support.

## 5.3 Ground Transport Simulations

### 5.3.1 Simulation Summaries

Four simulations were identified that could be applicable as tools in support of the TNFS$^2$ Program relative to the security of weapons being transported on the ground. Summary descriptions of these simulations are presented in the following subsections. These summaries indicate the type of simulation, the nature of the input data, the security system functions addressed, and the nature of the output data.

#### 5.3.1.1 Schaffer's Ambush Model

The Schaffer Ambush Model is a mixed Lanchester linear/square-law attrition simulation that is representative of the many Lanchester-type simulations that could be used to evaluate the outcomes of transport vehicle ambushes. The simulation assumes that an ambusher force is in concealed positions and initiates a surprise attack when the ambushee force arrives in a "killing zone." The ambushers' initial fire is aimed (Lanchester square law), while the ambushees initially react with area fire (Lanchester linear law). As the ambushees locate cover and begin to detect ambusher fire locations, they gradually switch from area to aimed fire. The ambushers maintain aimed fire throughout the engagement, although its effectiveness decreases as the engagement progresses. Ambushee desertions and ambusher withdrawals are considered in the simulation, and supporting weapons for the ambusher can also be included. For the initial surprise attack, the use of claymores is also an option.

The inputs to the simulation are the characteristics and effectiveness parameters representing each force. The inputs include the respective force sizes, weapon firing rates, single-round radial dispersion, and constants associated with troop discipline (used to determine desertion and withdrawal rates). Ambushee peculiar inputs are the speed at which an ambushee can approach the level of maximum cover, an individual's presented area at the beginning of the ambush, and the rate at which an individual can shift from area to aimed fire. The ambusher peculiar inputs are the average kill probability of a claymore and the total area occupied by the ambushers. Other inputs include the minimal final presented area of an individual under concealment, the probability of a kill given a hit, and the maximum time of the engagement--that is, the time at which the ambushers will withdraw in force.

The simulation is based on a time-stepped numerical integration (Runge-Kutta-Gill) of the two simultaneous Lanchester differential equations. The outputs of the simulation are the force sizes of the respective forces and the ambushee-ambusher force ratio at the end of the engagement. These output values can also be printed out at specified times during the engagement.

This aggregated simulation addresses the delay and neutralization functions of a security system. The documentation provides a derivation of the Lanchester equations, but does not include a program listing. However, a FORTRAN listing of a similar program is contained in another report (Ref. 114).

#### 5.3.1.2 SOURCE

The SOURCE code is a time-stepped Monte Carlo simulation developed by Sandia Laboratories to evaluate the initial stages of an ambush of a nuclear material transport convoy. This simulation considers the effects of the ambusher's fire, but does not simulate return fire from the convoy personnel.

The inputs to the simulation include a number of convoy characteristics. These are the maximum convoy length, the number of vehicles and their positions, vulnerable areas, the initial velocity, a visual observation distance, an emergency signal delay time, and the convoy tactics (escorts rendezvous with transport vehicle, vehicles attempt to escape from ambusher's field of fire, or combinations of both). The ambusher inputs are the number of attack units, their deployment, the unit initiating the ambush and its selected target, the initial open-fire distance, and the weapon characteristics (accuracy, maximum firing range, time between rounds, rounds per load, and reload time).

The simulation essentially begins when the target vehicle comes within the open-fire distance of the ambush initiating unit or within a prescribed observation distance of a roadblock. After this, other attack units open fire when a vehicle comes within range. Vehicles detect (and correctly assess) the attack either when fired upon or when they come within the visual observation distance of a roadblock or another vehicle being fired upon. The simulation allows for three communications channels--two regular and one emergency. Periodic communications are assumed on the regular channels, with the responsibility rotating in a fixed manner between the vehicles. An emergency message can also be sent by a vehicle under attack or by a vehicle that detects another vehicle under attack. The capability of sending a message depends on the condition of the crew and the communications equipment within a vehicle after the emergency signal delay time. A code is included in the simulation that describes the vulnerability of the vehicles and crew to the attacker's weapons, which includes the cumulative effects of multiple hits. The effects of the weapon firings on the crew and vehicles are determined by Monte Carlo sampling. The simulation assumes that the driver of a vehicle is the primary target and co-driver the secondary target. Vehicles are assumed to decelerate as vehicle damage is sustained. Survivability of the crew and vehicles is the only delay mechanism, in addition to escape, that is represented in the simulation. The engagement continues until a prespecified engagement time has elapsed.

The output of the simulations is the expected values of a number of output parameters, printed out at equal time increments during the engagement duration. These output parameters are the number of convoy personnel surviving, the number of convoy vehicles surviving and their locations, and the number of emergency signals generated.

The SOURCE simulation is an aggregated time-stepped Monte Carlo simulation that addresses the detection, assessment, communications, and delay functions of a security system. The program is coded in FORTRAN. The documentation provided presents a summary overview of the simulation, but does not include a program listing.

#### 5.3.1.3 SABRES*

The SABRES code is a time-stepped Monte Carlo simulation developed by Sandia Laboratories to evaluate the outcomes of engagements between attackers and defenders after a transport vehicle has been stopped. This simulation, developed to analyze the combat activities following the initial stages of an ambush, is used in conjunction with the SOURCE code (described in the previous subsection) to analyze the complete ambush confrontation.

The inputs required by SABRES are fairly extensive and can be segregated into four classes of characteristics: environment, vulnerability, adversary, and defender. The environment inputs include the specification, in a computer-usable format, of the surrounding terrain and the prevailing weather. The terrain model used is a modification of the SLAF terrain routine (Ref. 105). The surrounding area is given

*SABRES was developed in two phases. This discussion includes the modifications done in the second phase, which resulted in the SABRES II simulation.

an x-y grid structure with elevation data. Features such as vegetation, terrain type, and linear local obstacles are broken into specific identifying classes, and polygons are used as overlays on the grid representing the locations of these terrain features. Weather inputs include parameters that affect speeds of movement and visibility conditions. The vulnerability inputs provide the conditional probabilities of various degrees of incapacitation given a hit and are specified for different parts of the human body, weapon used, and range from weapon to target. The adversary inputs include their initial positions, group objective, weapons and ammo carried, mobility status, initial movement routes, firing rules, and vehicle penetration time distributions. The defender inputs are their initial positions (obtained, say, from SOURCE), initial cover objectives, weapons and ammo carried, and engagement tactics.

At the beginning of a simulation run, it is assumed that the ambushed vehicle of the convoy has been stopped and the defenders are seeking cover. Detection of individual adversary-defender pairs is checked at each time step. Probability of detection is a function of the existence of line of sight, contrast, range, weather, visibility, suppression state, and cover (this subroutine is based on a modification of the SIAF detection routine), (Ref. 106). Detections are maintained until line of sight is broken. Individual and vehicle movements are updated at each t e step. Once detections are made, firings commence if targets are in range. For each round fired, a Monte Carlo test is made to determine if a target is hit, and if it is, the level of incapacitation incurred. Presented and vulnerable areas consider the cover available and the target individual's posture. Rounds fired for each player are accumulated, and weapon reloads are initiated when magazines are emptied. At certain points during a battle, special events will occur such as an adversary covering group arriving in position, an adversary penetration group arriving at the transport vehicle, or a defender escort vehicle arriving to join the conflict. At these points, some logic [illegible] in the simulation to alter tactics if prespecified survival [illegible] are satisfied. The simulation continues until certain disen- [illegible] criteria are satisfied. This may be a successful penetration of the transport vehicle, a high attrition of adversaries, or the arrival of a large group of response forces, to name a few. When one of these disengagement conditions occurs, the replication is terminated and appropriate outcome values are accumulated and stored. After a prespecified number of replications of the same attack situation have been run, the run is terminated and the desired output statistics are printed out.

The major program outputs for a series of replications of an ambush are the expected survivors on each side, the fraction of time each side is totally successful, and the expected battle time. Although not explicitly stated in the documentation, numerous other secondary outputs should also be readily available. For a single replication, the simulation can be run on an interactive basis. In this case, the initial conditions are set up by use of the interactive display; the ambush is then allowed to run for a short period of time after which the status is displayed at the terminal. The user can then change objectives of the individual players and let the ambush continue for another short time. This assessment and run feature provides good insight as to the dynamics of an ambush and should prove a very useful training device for guard personnel.

The simulation addresses the delay and neutralization functions of a security system. The SOURCE/SABRES simulation combination then covers all six of the security system functions. The simulation is written in FORTRAN and can be run in batch mode or in an interactive mode on a timesharing system. Only overview documentation is presently available, although a user's manual is presently being written.

#### 5.3.1.4 TSEM

The Transportation Safeguards Effectiveness Model is a simulation developed by The BDM Corporation, with guidance from Sandia Laboratories. This simulation is designed to evaluate the outcomes of ambush attempts by an adversary force against a defended ground transport convoy carrying critical cargo such as special nuclear material.

The inputs required for this simulation are virtually the same as those required by the SOURCE/SABRES combination described in the previous two subsections. One large difference is that a script procedure has been developed for use with TSEM that attempts to make the definition of the ambush tactics easier to spell out and understand. A script language has been designed (and is being modified) that provides the user with a set of commands that will allow the simulation to map out the intended course of an ambush. This simplifies some of the inner structure of the simulation where logic branches would be required to provide for alternative tactics. This, then, implies that SOURCE/SABRES and TSEM are of the same level of complexity. However, TSEM is an event-sequenced simulation, while SOURCE/SABRES is a time-step simulation. Both simulations use the same terrain procedures and make use of several other SIAF routines, with modifications. The functions performed by TSEM parallel those described for SABRES, although TSEM covers the initial portion of the ambush also.

There are two primary output provisions. The Replication Output is a printout of several replication statistics. For each replication, the program prints out the replication number along with the outcome of that replication (draw, defender win, attacker win), and the numbers of defenders and attackers killed and those sustaining major and minor wounds. The output also indicates the number of replications that the defender won, that the attacker won, and that were draws, together with the conditional average battle times for each category.

A second output provision is the capability of generating a movie of a replication of an ambush. This provides a dynamic view of the interactions taking place during a given replication. This is a convenient tool for ensuring that a script has been written properly, and also provides a useful training technique.

This simulation addresses all six of the security system functions. The simulation is written in FORTRAN in both batch and timesharing modes of operation, although the timesharing mode at present does not include all the options available in the batch mode. Although much documentation exists, including a design requirements document and a user's manual, this documentation only provides an overview of the inner structure of the simulation.

### 5.3.2 Discussion

The simulations summarized in Section 5.3.1 above indicate the state of the art in ground transport security system simulation modeling. Although these simulations are lacking in several areas, effort is proposed or in progress to expand or modify the detailed simulations to more fully address the spectrum and scope of the confrontation situations addressed. Vector Research, Inc. is also providing support to Sandia Laboratories in developing an alternative ground transport simulation, identified as CONVOY in a recent progress report (Ref. 43). Thus, as with the fixed site security system simulations, development effort is still being undertaken to expand the state of the art.

The discussion will now address the six simulation characteristics identified in Section 4.3.

#### 5.3.2.1 Completeness

The simulations summarized in this section all address an ambush confrontation situation. The aggregated Schaffer Ambush Model is a one-force-on-one-force simulation, in that the ambushers all have the same objective--that of destroying the ambushee force. The simulation was designed for use with an on-foot ambushee force, so it really does not address a ground transport situation. However, a set of routines along this line operating in parallel could provide an aggregated substitute for the SABRES simulation, which addresses the ambush at the time when vehicle personnel seek out cover. The SOURCE/SABRES combination and the TSEM simulations both are fairly detailed simulations that address the ambush of a truck convoy. Both of these simulations assume a well-concealed ambush force where detection by the convoy is based on either the observance of a roadblock or the awareness of ambusher fire. No consideration is given to the possible pre-ambush detection by an accompanying reconnaissance helicopter or by a leading escort vehicle that could allow a weapon transport vehicle to alter its route in order to avoid the ambush. Although this situation might be included in a TSEM input script, it would be a deterministic event and would not be very useful in evaluating the effectiveness of reconnaissance in enhancing ground transport security. These simulations also do not address the airmobile force attack situation. In addition, the simulations at present do not directly include the arrival of response forces and their integration in the battle, although indirectly a distant trailing vehicle of the convoy could be programmed as a response force with zero velocity movement until an alarm is given by one of the other convoy vehicles.

The SOURCE/SABRES combination simulation and the TSEM simulation do address all six of the security system functions, but in light of the above, they are both deficient in the detection function (no pre-ambush detections) and neutralization function (no direct response force inclusion).

#### 5.3.2.2 Dual Complexity

None of the simulations discussed possesses a dual complexity characteristic at present.

#### 5.3.2.3 Modularity

The Schaffer Ambush Model is a single module unto itself. It could serve as one module in a more comprehensive, though still aggregated, simulation that addresses several skirmishes, in addition to the detection, assessment, and communication functions. The documentation on the SOURCE/SABRES combination and TSEM simulation does not provide program listings, but infers that these simulations are modular in nature and that the modular breakdown is sufficient to group modules in accordance with the individual security system functions.

#### 5.3.2.4 Test Compatibility

The wide variety and detail of the inputs required by both the SOURCE/SABRES combination and the TSEM simulation provide for excellent compatibility with TNFS$^2$ Program requirements. Although some of the simulation inputs may have to be derived from the test input parameters, this is much more the exception than the rule. On the output side, it is apparent that modifications in the output structures of the simulations will be required to provide convenient structures for comparing simulation results with test results on a security system function level. The Schaffer Ambush Model is essentially not compatible with the requirements of the TNFS$^2$ Program.

#### 5.3.2.5 Machine Independence

The programming language of all the simulations summarized in this section is FORTRAN and should not be a problem in transferring the programs to another computer system. Both the SOURCE/SABRES combination and the TSEM simulation appear to have extensive data files. The documentation does not specify whether or not these data files are constructed in a machine-dependent manner. If they are, then some effort would have to be devoted to restructuring these files to ensure compatibility with the appropriate computer system.

#### 5.3.2.6 Usability

All of the simulations summarized in this section require the establishment of a data base. Once this data base is established, the use of the simulations appears to be straightforward, although for the TSEM simulations, above-normal training may be required to obtain the faculty to rapidly generate the input scripts. Although an estimate of two to three days for script generation is reasonable, these could be prepared ahead of time and thus not be a problem for near-real-time support of test operations. Documentation relative to the Schaffer Ambush Model is adequate, but the existing documentation for the SOURCE/SABRES combination and TSEM simulation is not sufficient in its present form.

A user's manual is presently being written for the SABRES simulation, and one is already available for the TSEM simulation. The latter, however, is strictly a user's manual and does not provide any information as to the inner structure of the simulation, so additional documentation is also needed. From the description of all the simulations, running time does not appear to be a problem for near-real-time support.

## 5.4 Air Transport Simulations

### 5.4.1 Simulation Summaries

Two simulations were identified that could provide some insights into the development of simulation tools in support of the TNFS$^2$ Program relative to the security of weapons being transported by air. Summary descriptions of these simulations are presented in the following subsections. These summaries indicate the type of simulation, the nature of the input data, the security system functions addressed, and the nature of the output data.

#### 5.4.1.1 PENAIR

The PENAIR simulation is a time-stepped stochastic simulation developed to evaluate the effectiveness of alternative defensive tactics for an unarmed aircraft while overflying hostile terrain. The simulation is limited to a single aircraft, but allows up to a maximum of 200 ground weapons (limited to 10 different types).

The terrain is simulated by defining polynomial functions of two independent variables (x, y) to values of a dependent variable (h) specified at points on an x-y rectangular grid. The grid rectangle can be divided into up to 12 grid squares, and each square is assigned a polynomial grid function. A separate computer program, TERRAIN, is used to generate the polynomials from a finer grid of real terrain data. For the simulation, the inputs include the number of rectangles used, the degrees in x and y of the associated polynomials, and the respective polynomial coefficients. The inputs for the ground weapons, include, for each weapon type, the number of weapons and their locations, the time required to acquire the target, firing time before reloading, time required to reload, minimum and maximum weapon ranges, and the probability of a kill by the weapon at various slant ranges (20 maximum) during a simulation time-step period. The aircraft inputs include the maximum positive g's to be used by the aircraft, maximum rates of climb and descent, estimated ground speed, starting position (assumed in-flight), and objective coordinates.

The aircraft's flight path can be specified in three different ways. First, a pre-planned flight path can be specified by input. Second, a straight-line flight path, in the horizontal plane, can be assumed and the simulation will generate a nap-of-the-earth flight path in altitude. The third type of flight path assumes a straight and level flight until a ground weapon commences firing on the aircraft. The aircraft can then execute one of 18 evasive maneuvers. These 18 maneuvers consist of six basic maneuvers with three possible speed choices for each basic maneuver. The speed choices are increase speed, decrease speed, or maintain speed. The six basic maneuvers are: (1) continue flying straight ahead at the same altitude, (2) commence a climb straight ahead at the aircraft's maximum rate of ascent, (3) turn away from the weapon remaining at the same altitude, (4) turn away and commence a maximum rate climb, (5) dive for the deck and commence nap-of-the-earth flight straight ahead, or (6) turn away from the weapon, dive for the deck, and commence nap-of-the-earth flight.

The simulation begins by moving the aircraft along its flight path in accordance with unit time-step intervals. For each time-step interval, the existence of line of sight between the aircraft and each weapon is determined. Once the aircraft has been within continuous LOS with a weapon for a period of time equal to the acquisition time, it is assumed that the weapon has detected the target and can commence firing, provided the aircraft is within the range limits and the weapon is loaded. A weapon, once it commences firing, will fire until it must reload, until it loses line of sight with the aircraft, or until the aircraft escapes from the weapon's range limits. Once a weapon commences firing on the aircraft, the aircraft (if given a maneuver option) begins executing the intended escape maneuver. At each time-step interval in which there are weapon firings, the aircraft's survivability is degraded in accordance with single-time interval survival probabilities relative to those weapon firings. The simulation continues in this manner until the aircraft completes its flight path or it flies out of the area covered by the terrain grid.

The primary outputs of the simulation are the survivability results and the flight-path map. The survivability results include the total aircraft survivability and, for each weapon, the total time in view and the aircraft's survivability against that weapon. The flight-path map is a chronological listing of the aircraft's (x, y, h) coordinates. These can be used to plot a graph of the aircraft's flight path in the (x, y) plane and also a graph of the flight path in elevation with a terrain elevation overlay.

This is a fairly aggregated, combined deterministic-stochastic simulation that addresses the detection, assessment, and delay functions of a security system. It is written in FORTRAN (an obsolete version, though). The documentation is excellent, with flowcharts and listings of all the routines. The auxiliary program TERRAIN is also described and a program listing provided.

#### 5.4.1.2 Armed Escort Model

The Armed Escort Model is a time-stepped, Monte Carlo simulation developed by Electronic Associates, Inc. to evaluate the effectiveness of an armed escort helicopter in protecting a formation of troop-carrying helicopters against a single ground weapon, where the ground weapon is located in near proximity to the lift aircraft's landing zone.

The simulation inputs are quite extensive and can be segregated into four categories: escort aircraft data, formation data, ground weapon data, and vulnerable area data. The escort aircraft inputs include coefficients for a recognition delay equation, which depends on the aircraft position, orientation, and gun turret rotation, if applicable. The escort aircraft's flight path, including orientation and velocity, is specified as input, as are the aircraft's weapon system properties such as rate of fire and single round probability of defeating a man at the ground weapon as a function of time along the flight path. The formation inputs include the flight path of the leader lift aircraft, including orientation and velocity, and the relative positioning of the other lift aircraft with respect to the leader. Other inputs include smoothing constants, heading limits for ground weapon fires, and maximum hover velocity (when velocity drops below maximum, the aircraft are committed to a landing approach). The ground weapon inputs include its location, minimum and maximum firing range, visibility range, rate of fire, ammo load, acquisition delay time, defeat delay time, assessment delay time, reload delay time, and replacement delay time. This latter delay time refers to the time required for a reserve gunner to move up from a reserve position to replace a gunner defeated at the weapon. Other related inputs include the number of gunners at the weapon and in reserve, and the minimum number required at the weapon for it to be functional or suppressed (weapons are defeated only through defeating the attending gunners). Other ground weapon inputs include constants for a linear projectile velocity equation, which is a function of range. The vulnerability inputs include vulnerable areas on the two types of aircraft in terms of front, side, rear, and bottom views. The vulnerable areas are broken down into components that reflect different damage conditions: mechanical attrition, forced landing, mission abort, pilot attrition, co-pilot attrition, forced landing, mission abort, pilot attrition, co-pilot attrition, engine attrition or troop attrition, and some selected combinations of the above such as both pilot and co-pilot attrition. These vulnerability inputs also include impact velocity breakpoints for each vulnerable area component.

A simulation replication begins by moving the aircraft along their flight paths in time-step increments. At each step, a test is made to determine if an aircraft is within visibility range of the ground weapon. If yes, then the ground weapon selects the more favorable in-range target to fire on (firing escort aircraft has highest priority). If some gunners have been defeated, then reserves are moved a time-step closer to the weapon. If the weapon is defeated or reloading, or the target is unacquired, the delay counters are decremented. Otherwise, the weapon fires at the target aircraft (if lift aircraft, then only if aircraft is in hover). Aircraft attrition is then evaluated and if the aircraft is attrited, a ground weapon assessment delay counter is initiated. Ammo supply is checked and reload delay initiated if supply is expended. If the ground weapon has commenced firing at this time or before, the escort will begin firing when ready to fire (in range and at the proper orientation). If the escort fires, then ground damage is evaluated. If the weapon is defeated, a defeat and acquisition delay is initiated. At this point, the simulation proceeds to the next time step and the procedure is repeated. This continues until the ground weapon, including reserves, has been defeated, all aircraft have exited from visibility range of the ground weapon, or a game time limit has been exceeded.

After a specified number of replications have been processed, the results are accumulated and output statistics are computed. These output statistics are the means and standard deviations of the probability distributions for aircraft damage. The expected number of aircraft in each damage state is also given, as are the expected fractions of lift aircraft attritions and ground personnel attritions.

This simulation is a very detailed, combined deterministic-stochastic, Monte Carlo simulation that addresses the detection, assessment, delay, and neutralization functions of a security system. The program is written in FORTRAN. The documentation is excellent and includes flowcharts and a complete program listing.

### 5.4.2 Discussion

The simulations summarized in the preceding section are not, per se, directly applicable to providing simulation support to the $TNFS^2$ Program. However, they do provide some insight that will be helpful in the development of appropriate simulation tools. The PENAIR simulation allows an aircraft (weapon transporter) to maneuver to escape from the ground-based attackers, but does not include escort aircraft and their suppressive effects. The Armed Escort Model, on the other hand, considers the suppressive and destructive effects of escorts on the attacking weapon, but does not allow the cargo-carrying aircraft to deviate from their original flight paths. A combination of the functions addressed by the two simulations would result in a simulation approach that would be more applicable to the TNF weapon air-transport situation where a transport aircraft is normally accompanied by an armed escort aircraft.

Since neither of the simulations is directly applicable to the $TNFS^2$ Program requirements, a detailed discussion of their attributes relative to the six simulation characteristics identified in Section 4.3 is not in order. Both simulations are over ten years old and programmed in obsolete versions of FORTRAN. However, the documentation for each simulation is more than adequate and should prove useful in future development work.

## 5.5 Input Data Availability

The usefulness of simulations is limited by the quality and quantity of input data that is available. By the nature of the inputs involved, it is apparent that each of the simulations summarized in Sections 5.2, 5.3, and 5.4 above were designed in accordance with available or soon-to-be-available data inputs. During the development of the fixed site and ground transport simulations in the past few years, a concerted parallel effort has also been undertaken by Sandia Laboratories, among others, to establish as complete a data base as possible relative to security systems and components. Contractual efforts with SRI International, Applied Psychological Services, and Vector Research, Inc. together with Sandia's own efforts have generated broad data bases in such areas as Barriers, Intrusion Detection, Duress Alarm Activation, Alarm Communications and Displays, Entry Control, Assessment, Communications, Small Arms Weapons Characteristics, and Human Performance. This concerted effort has resulted in the accumulation, categorization, and filing of a vast amount of reliable input data. The results of this work also include the identification of areas where reliable input data do not exist. Some testing has already been proposed and is possibly in progress in an attempt to bridge some of the gaps. Additional testing, including that to be conducted under the TNFS$^2$ Program, will produce additional data to narrow the gaps in the data bases. In developing simulation tools for the program, care should be taken to ensure that the simulation designers are knowledgeable as to the contents and voids in the appropriate data bases.

## 5.6 Conclusions

Based on the results of this research effort, there are a number of conclusions that can be drawn with respect to the availability of simulation tools that would be directly applicable to the TNFS$^2$ Program. Some of these hold in general, while others are directed specifically to Fixed Site Simulations, Ground Transport Simulations, or Air Transport Simulations. These conclusions are as follows:

- General
  - Simulations developed for purposes other than security system evaluation are not, in general, easily adaptable for the purpose of security system evaluation.
  - Simulations developed for the purpose of security system evaluation do provide an adequate base of departure for the development of TNF security system evaluation simulations.
  - The simulations reviewed are directed to a single weapon state (fixed site, ground transport, or air transport) and thus do not address the transitional operations involved in going from one state to another.
  - For the purposes of the TNFS$^2$ Program, a significant amount of simulation development activity will be required, especially if the Dual-Complexity characteristic (discussed in Section 4) is desired.
  - Sandia Laboratories has amassed a broad security system data base that will be of use for the TNFS$^2$ Program. Users, though, should be knowledgeable as to the existing data voids.
- Fixed Site Simulations
  - The Forcible Entry Safeguards Effectiveness Model (FESEM) developed by Sandia Laboratories is one simulation that

is directly applicable to TNF security system evaluation. Some modification and expansion will be required. The program uses the FORTRAN-based GASP-IV simulation language, which may pose some minor problems in transferral to an alternate computer system.

- The VISA methodology developed by Science Applications, Inc. provides an alternative approach to FESEM. This would also require some modification for TNF security system evaluation purposes. A network simulation program utilizes the FORTRAN-based Q-GERT queueing network simulation language, which could pose problems.
- Desirable features of both FESEM and VISA could be combined to provide for an initial baseline simulation to build on for TNF security system evaluation purposes.
- Sandia Laboratories aggregated model EASI (Estimate of Adversary Sequence Interruption) is too aggregated even for use as an aggregated simulation in support of the TNFS$^2$ Program. Furthermore, it does not consider the neutralization function.
- None of the fixed site simulations reviewed address the problem of false detections and false alarms.
- None of the detailed or aggregated infantry combat simulations surveyed appear to be directly useful for fixed site security system evaluations.

• Ground Transport Simulations

- The SOURCE/SABRES simulation combination developed by Sandia Laboratories is one set of simulations that is directly applicable to TNF security system evaluation, although some modification and expansion will be required.
- The TSEM (Transportation Safeguards Effectiveness Model) developed for Sandia Laboratories by the BMD Corporation is another simulation directly applicable to TNF security system evaluation requirements. Some modification will also be required.
- Most of the infantry combat simulations do not appear directly applicable for the TNFS$^2$ Program requirements. The SABRES and TSEM simulations make use of some of the better subroutines of these combat simulations.
- As an aggregated simulation, Schaffer's Ambush Model may be useful for TNF security system evaluation purposes. However, it would have to be broadly expanded for this purpose.

• Air Transport Simulations

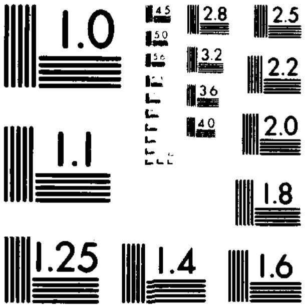
- No adequate simulation was uncovered that would be directly applicable for this case.

AD-A089 696 SRI INTERNATIONAL MENLO PARK CA F/G 15/3
AN ASSESSMENT OF AVAILABLE SECURITY SYSTEM SIMULATIONS TO SUPPO--ETC(U)
FEB 79 R H MONAHAN, E L DUBOIS DNA001-78-C-0321

UNCLASSIFIED DNA-4886F NL

2 of 2
AD A089696

END
DATE FILMED
11-80
DTIC


1.0
4.5
5.0
5.6
2.8
2.5
3.2
2.2
3.6
4.0
2.0
1.1
1.8
1.25
1.4
1.6

- Most air-oriented simulations either are one-on-one simulations for evaluating air defense weapon effectiveness against fixed and rotary wing aircraft or are simulations for evaluating the effectiveness of attack helicopters in support of ground combat operations. However, some selected subroutines may be of use in the development of an air transport simulation for use in the TNFS$^2$ Program.

# SECTION 6

# FUTURE SIMULATION TOOLS DEVELOPMENT PROGRAM

The results of the analysis of the availability of simulation tools indicate that a significant amount of simulation development effort will be required to establish a viable simulation capability to support the TNFS$^2$ Program. The implementation of such a program should take maximum advantage of existing assets and expertise in order to conserve time, effort, and funds, without sacrificing the quality of the final products. In order to achieve this objective, a seven-task program is recommended. The interrelationships among the tasks are indicated in Figure 6.1. A brief discussion of each task is presented below.

## 6.1 Task 1--Simulation Tools Development Plan

The purpose of this task is to establish a detailed plan for the development of the appropriate simulation tools to support the TNFS$^2$ Program. This plan should be based on a detailed analysis of the objectives and scope of the test program. This analysis should delineate the specific scenarios of concern, the levels at which testing will be conducted, the areas in which the simulations will complement the testing, the desired levels of simulation complexity (including the desirability for a dual complexity approach), and other related factors. The results of this analysis should provide for the establishment of detailed task descriptions for the five simulation development tasks.

## 6.2 Task 2--Simulation Tools Development Program Technical Management

This task is directed to all the activities required to provide technical management in the conduct of the simulation tools development program. Initially this task will involve providing technical advice in the selection of performers for the work required in each of the five

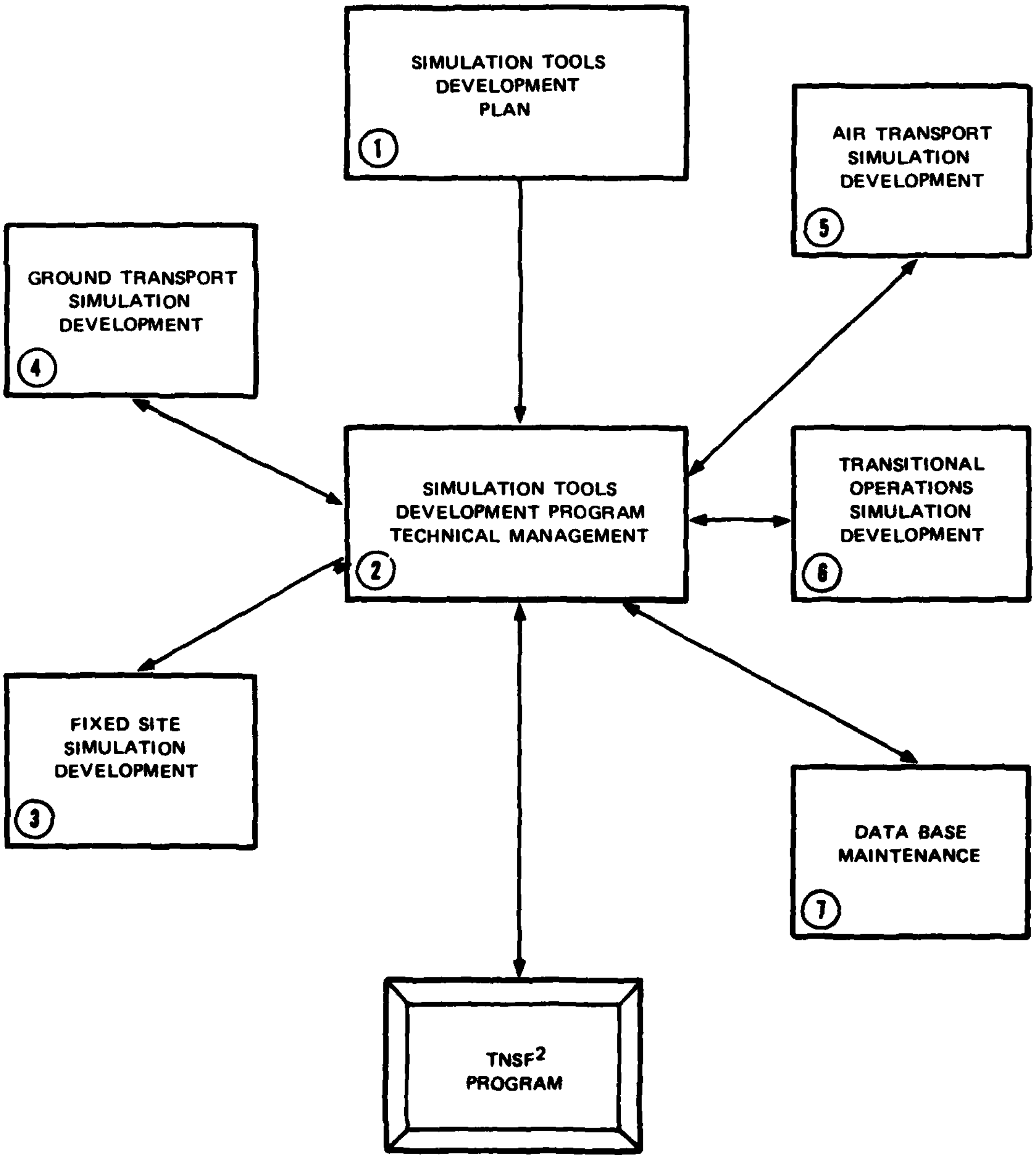

SIMULATION TOOLS DEVELOPMENT PLAN
1
AIR TRANSPORT SIMULATION DEVELOPMENT
5
GROUND TRANSPORT SIMULATION DEVELOPMENT
4
SIMULATION TOOLS DEVELOPMENT PROGRAM TECHNICAL MANAGEMENT
2
TRANSITIONAL OPERATIONS SIMULATION DEVELOPMENT
6
FIXED SITE SIMULATION DEVELOPMENT
3
DATA BASE MAINTENANCE
7
TNSF2 PROGRAM

FIGURE 6-1 SIMULATION TOOLS DEVELOPMENT PROGRAM--TASK INTERRELATIONSHIPS

simulation development tasks. Subsequent effort will be devoted to technical monitoring of the performer efforts, providing integration among the individual performers, maintaining liaison with the test program activities, and performing any other duties required to ensure that the program runs smoothly and on schedule.

## 6.3 Task 3--Fixed-Site Simulation Development

This task is directed to the development of a fixed site simulation to be used in support of testing activities to evaluate the effectiveness of security systems for weapons located at temporary or permanent storage sites. The requirements of this simulation will be detailed in the Simulation Tools Development Plan. The development activities should make maximum use of the fixed site simulations that are available today. To avoid unnecessary duplication of effort and to draw upon previous experience in such simulation development, the performer should be selected from those who already have an existing fixed site simulation capability.

## 6.4 Task 4--Ground Transport Simulation Development

This task is directed to the development of a ground transport simulation to be used in support of testing activities to evaluate the effectiveness of security systems for weapons being transported via ground transportation. The requirements of this simulation will be detailed in the Simulation Tools Development Plan. The development activities should make maximum use of the ground transport simulations that are available today. To avoid unnecessary duplication of effort and to draw upon previous experience in such simulation development, the performer should be selected from those who already have an existing ground transport simulation capability.

## 6.5 Task 5--Air Transport Simulation Development

This task is directed to the development of an air transport simulation to be used in support of testing activities to evaluate the effectiveness of security systems being transported by air. The requirements of this simulation will be detailed in the Simulation Tools Development Plan. The development activities should make maximum use of existing expertise in the area of ground versus air simulations. Thus, the performer should be selected from those agencies having both expertise in this simulation area and a strong background in security system operations.

## 6.6 Task 6--Transitional Operations Simulation Development

This task is directed to the development of a set of simulations that address the transitional operations involved in transferring TNF weapons from one weapon status state to another and can be used in support of testing activities to evaluate the effectivnesss of security systems during these transitional periods. The requirements for these simulations will be detailed in the Simulation Tools Development Plan. Since these simulations will be connecting links between the other simulations being developed in this program, continuity of effort should be maintained as much as possible. One way to ensure this is to assign the development effort for each particular simulation out of this set of simulations to one of the performers developing a pure status state simulation that involves one of the associated weapon status states.

## 6.7 Task 7--Data Base Maintenance

This task is directed to the establishment and maintenance of an appropriate data base to be used in support of the simulations being developed under this program. The nature of the data to be collected and maintained will be specified in the Simulation Tools Development Plan. The detailed data requirements will be initially established from preliminary simulation designs submitted by the simulation development performers. These data requirements will then be continuously updated as the development of the simulations progresses and as additional data become available from testing programs and other sources. To avoid unnecessary duplication of effort and to draw upon previous experience in security system data base maintenance, the performer should be selected from those who have existing security system data bases.

# REFERENCES

1. DoD Directive 4540.3, "Logistic Movement of Nuclear Weapons" (19 December 1972).

2. DoD Directive 5030.15, "Safety Studies and Reviews of Nuclear Weapons Systems" (8 August 1974).

3. DoD Directive 5210.41, "Security Criteria and Standards for Protecting Nuclear Weapons" (10 September 1976).

4. DoD Directive 5100.76, "Physical Security Review Board" (17 May 1977).

5. DoD Instruction 4540.4, "Safety Standards and Procedures for the Logistic Movement of Nuclear Weapons" (20 December 1972).

6. DA, FM 19-30, Physical Security (November 1971), with Change 1 (30 January 1975) and Change 2 (29 August 1975).

7. DA, FM 6-20, Field Artillery Tactics and Operations (August 1973).

8. DA, FM 100-50, Nuclear Unit Operations in Combat (31 March 1977).

9. DA, FM 5-26, Employment of Atomic Demolition Munitions (ADM) (August 1971).

10. DA, FM 9-47, Special Ammunition Unit Operations (October 1970).

11. DA, AR 50-5, "Nuclear and Chemical Weapons and Materiel--Nuclear Surety" (15 July 1976).

12. DA, TM 39-45-51, Transportation of Nuclear Weapon Materiel (22 January 1976), with changes through 2-3 (25 March 1977).

13. DA, FM 55-15, Transportation Reference Data (February 1968).

14. DA, FM 1-100, Army Aviation Utilization (18 August 1969).

15. DA, FM 101-20, U.S. Army Aviation Planning Manual (February 1976).

16. DA, TM 5-225, Radiological and Disaster Recovery at Fixed Military Installations (June 1966).

17. DA, FM 101-31-1, Staff Officers' Field Manual--Nuclear Weapons Employment Doctrine and Procedures (February 1968).

18. DARCOM, "Nuclear Surety Program--Reference List" (December 1976).

19. DARCOM, Supplement 1 to AR 50-5, "Nuclear Weapons and Materiel--Nuclear Surety" (10 September 1976).

20. CIA, Research Study, International and Transnational Terrorism: Diagnosis and Prognosis, PR 76 10030 (April 1976).

21. U.S. Department of Justice, Law Enforcement Assistance Administration, Facing Tomorrow's Terrorist Incident Today (October 1977).

22. M. Willrich and T. B. Taylor, Nuclear Theft: Risks and Safeguards, Ballinger Publishing Co., Cambridge, MA (1974).

23. D. Carlton and C. Schaerf, eds., International Terrorism and World Security (Croom Helm, Ltd., London, 1975).

24. J. Record and T. I. Anderson, U.S. Nuclear Weapons in Europe--Issues and Alternatives (The Brookings Institution, Washington, D.C., 1974).

25. E. B. Baker et al., "Development of Hybrid Computer Programs for AAFSS/COBRA/COIN Weapons Effectiveness Studies. Volume 1. Simulating Aircraft Maneuvers and Weapon Firing Runs," TR-ECOM-0241-F1, Final Report, Electronic Associates Inc., Princeton, NJ (September 1968).

26. E. B. Baker et al., "Development of Hybrid Computer Programs for AAFSS/COBRA/COIN Weapons Effectiveness Studies. Volume 4. Monte Carlo Simulation of a Tactical Engagement Between Air and Ground Forces," TR-ECOM-0241-F4, Final Report, Electronic Associates Inc., Princeton, NJ (October 1968).

27. H. A. Bennett, "The 'EASI' Approach to Physical Security Evaluation," Report No. SAND76-0500, Sandia Laboratories, Albuquerque, NM (January 1977).

28. D. W. Sasser, "EASI on the HP-25, HP-65, and HP-67," Report No. SAND76-0597, Sandia Laboratories, Albuquerque, NM (May 1977).

29. H. A. Bennett, "User's Guide for Evaluating Physical Security Capabilities of Nuclear Facilities by the EASI Method," Report No. SAND77-0082, Sandia Laboratories, Albuquerque, NM (June 1977).

30. D. W. Sasser, "Users Guide for EASI Graphics," Report No. SAND78-0112, Sandia Laboratories, Albuquerque, NM (March 1978).

31. L. D. Chapman, "Effectiveness Evaluation of Alternative Fixed-Site Safeguard Security Systems," Report No. CONF-760703-5, Sandia Laboratories, Albuquerque, NM (1976).

32. L. D. Chapman et al., "Users Guide for Evaluating Alternative Fixed-Site Physical Protection Systems Using FESEM," Report No. SAND77-1367, Sandia Laboratories, Albuquerque, NM (November 1977).

33. L. D. Chapman, "Fixed-Site Physical Protection System Modeling," Report No. CONF-751283-1, Sandia Laboratories, Albuquerque, NM (1975).

34. B. L. Hulme, "Graph Theoretic Models of Theft Problems. I. The Basic Theft Model," Report SAND75-0595, Sandia Laboratories, Albuquerque, NM (November 1975).

35. B. L. Hulme, "Pathfinding in Graph-Theoretic Sabotage Models. I. Simultaneous Attack by Several Teams," Report SAND76-0314, Sandia Laboratories, Albuquerque, NM (July 1976).

36. B. L. Hulme and D. B. Holdridge, "KSPTH: A Subroutine for the K Shortest Paths in a Sabotage Graph," Report No. SAND77-1165, Sandia Laboratories, Albuquerque, NM (August 1977).

37. S. E. Jacobsen, "Optimal Improvement of Graphs Related to Nuclear Safeguards Problems," Report No. SAND76-0435, Sandia Laboratories, Albuquerque, NM (October 1977).

38. B. L. Hulme, "MINDPT: A Code for Minimizing Detection Probability Up to a Given Time Away from a Sabotage Target," Report No. SAND77-2039, Sandia Laboratories, Albuquerque, NM (December 1977).

39. "Monte-Carlo Approach to the Generation of Adversary Path," Report No. CONF-771109-30, Sandia Laboratories, Albuquerque, NM (1977).

40. J. L. Harrison, "A Computer Simulation of an Aircraft Penetration Over Hostile Terrain," Master's Thesis, Naval Postgraduate School, Monterey, CA (1965).

41. S. C. Keeton and P. Laquil, III, "Conflict Simulation for Surface Transport Systems," Report No. CONF-770656-23, Sandia Laboratories, Albuquerque, NM (July 1977).

42. R. J. Gallagher et al., "The Evaluation of Road-Transit Physical Protection Systems," Report No. SAND78-8650, Sandia Laboratories, Livermore, CA (July 1978).

43. L. D. Chapman, "Physical Protection of Nuclear Material in Transit," Quarterly Progress Report, April-June 1978, SAND78-2043, Sandia Laboratories, Albuquerque, NM (December 1978).

44. N. Salikupta, "A Factorial Parameter Analysis of Schaffer's Ambush Combat Model," Master's Thesis, Naval Postgraduate School, Monterey, CA (September 1974).

45. R. J. Wagner et al., "Configuration of Road Convoys: A Simulation Study," Report No. CONF-770656-22, Sandia Laboratories, Albuquerque, NM (July 1977).

46. "Transportation Safeguards Systems Support--Task 4 Final Technical Report," BMD/A-77-057-TR, The BDM Corporation, Albuquerque, NM (March 1977).

47. "TSEM Preliminary Design-Functional Specification," BMD/A-77-264-TR, The BDM Corporation, Albuquerque, NM (June 1977).

48. "TSEM Phase II User's Manual," BMD/TAC-78-253-TR, The BDM Corporation, Albuquerque, NM (June 1978).

49. H. Donnelly et al., "A Method for Evaluating the Performance of Integrated Safeguards Systems at Nuclear Facilities, Volume I," NUREG-0317, Final Report, Science Applications, Inc., La Jolla, CA (August 1977).

50. H. Donnelly et al., "A Method for Evaluating the Performance of Integrated Safeguards Systems at Nuclear Facilities. Volume II. Appendices," NUREG-0317, Final Report, Science Applications, Inc., La Jolla, CA (August 1977).

51. H. E. Lambert and J. J. Lim, "The Modeling of Adversary Action for Safeguards Effectiveness Assessment," UCRL-79217, Rev. 1, Lawrence Livermore Laboratory, Livermore, CA (June 1977).

52. F. M. Gilman, H. E. Lambert, and J. J. Lim, "The Results of a Directed Graph and Fault Tree Assessment of a MC&A System," UCRL-80802, Lawrence Livermore Laboratory, Livermore, CA (June 1978).

53. H. E. Lambert, J. J. Lim, and F. M. Gilman, "Material Control Study: A Directed Graph and Fault Tree Procedure for Adversary Event Set Generation," UCRL-81823, Lawrence Livermore Laboratory, Livermore, CA (October 1978).

54. D. Thompson and L. Jacobi, "The Representation of Suppression in the TRASANA AIDM," Report No. BDM/CARAF-TR-049, BDM Services Co., Leavenworth, KS (21 April 1975).

55. "Analytic Models of Air Cavalry Combat Operations--Volume I," Final Report No. SAG-1-Vol-1, FR-73-1-Vol-1, Vector Research Inc., Ann Arbor, MI (May 1973).

56. "Analytic Models of Air Cavalry Combat Operations--Volume II," Final Report No. SAG-1-Vol-2, FR-73-1-Vol-2, Vector Research Inc., Ann Arbor, MI (May 1973).

57. J. H. Hawkins, "The AMSAA War Game (AMSWAG) Computer Combat Simulation," Technical Report No. AMSAA-TR-169, Army Materiel Systems Analysis Activity, Aberdeen Proving Ground, MD (May 1976).

58. D. Engi, "Small-Scale Engagement Model with Arrivals: Analytical Solutions," Report No. NUREG-0238, Sandia Laboratories, Albuquerque, NM (April 1977).

59. R. R. Johnson and N. R. Van Leeuwen, "A Simulation of Helicopter Aircraft in an Armed Reconnaissance Mode for the CDC 1604 Digital Computer," Master's Thesis, Naval Postgraduate School, Monterey, CA (May 1966).

60. J. Honig et al., "Review of Selected Army Models," Review Report, Department of the Army, Washington, D.C. (May 1971).

61. R. C. Adkins, "Analysis of Unit Breakpoints in Land Combat," Master's Thesis, Naval Postgraduate School, Monterey, CA (March 1975).

62. L. G. Gref and J. W. Rosengren, "An Assessment of Some Safeguards Evaluation Techniques," Report No. RDA-TR-5000-002, R&D Associates, Arlington, VA (February 1977).

63. W. Eckhardt and D. W. Mader, "CARMONETTE III Documentation," RAC-R-28, Volume I--General Description, Research Analysis Corp., McLean, VA (October 1967).

64. C. A. Bruce, Jr., et al., "CARMONETTE III Documentation," RAC-R-28, Volume II--Data-Preparation Guide, Research Analysis Corp., McLean, VA (February 1968).

65. N. W. Parsons et al., "The Use of CARMONETTE IV in Assessing the Combat Effectiveness of Small Units Equipped with Night Vision Devices," Final Report No. RAC-009.302, Research Analysis Corp., McLean, VA (November 1969).

66. N. W. Parsons, "CARMONETTE IV and CARMONETTE V," Report No. RAC-D12-CR, Research Analysis Corp., McLean, VA (October 1972).

67. G. S. Colonna and R. G. Williams, "CARMONETTE: Volume I--General Description," Report No. OAD-CR-73-Vol-1, General Research Corp., McLean, VA and Operations Analysis Division, Army Concepts Analysis Agency, Bethesda, MD (November 1974).

68. G. S. Colonna and R. G. Williams, "CARMONETTE: Volume II--Data Preparation and Output Guide," Report No. OAD-CR-73-Vol-2, General Research Corp., McLean, VA, and Operations Analysis Division, Army Concepts Analysis Agency, Bethesda, MD (November 1974).

69. R. G. Williams, "CARMONETTE: Volume III--Technical Documentation," Report No. OAD-CR-73-Vol-3, General Research Corp., McLean, VA, and Operations Analysis Division, Army Concepts Analysis Agency, Bethesda, MD (November 1974).

70. K. Thorp et al., "Comparison of the CARMONETTE Model with the TETAM Field Experiment," Report No. CAA-TP-75-6, Army Concepts Analysis Agency, Bethesda, MD (September 1975).

71. R. Zirkind and R. E. Forrester, "Tactical Electrooptical Effectiveness Model, Phase II--Volume I," Report No. CR-191, General Research Corp., McLean, VA (June 1977).

72. J. R. Penick, "Optical Threat/Laser Countermeasures Engagement Analysis," Report No. AFIT/GEP/PH/77-10, Air Force Institute of Technology, Wright-Patterson AFB, OH (December 1977).

73. D. E. Christy, "A Lanchester Based Model for Analyzing Infantry Fire and Maneuver Tactics," Master's Thesis, Naval Postgraduate School, Monterey, CA (October 1969).

74. A. B. Bishop and S. Stellmack, "The Tank Weapon System: Vol. I--Design Models," Report No. RF-573 AR 68-1 (U), Systems Research Group, Ohio State University, Columbus, OH (September 1968).

75. A. B. Bishop and G. M. Clark, "The Tank Weapon System: Vol. II--Design of Operations Models," Report No. AR 69-2A, Systems Research Group, Ohio State University, Columbus, OH (1969).

76. G. M. Clark and L. C. Moss, "The Tank Weapon System: Vol. III--DYNTACS Computer Program," Report No. AR 69-3A, Systems Research Group, Ohio State University, Columbus, OH (June 1969).

77. A. B. Bishop and G. M. Clark, "The Tank Weapon System: Vol. IV--Summary," Report No. AR 69-4, Systems Research Group, Ohio State University, Columbus, OH (1969).

78. G. M. Clark and S. H. Parry, "Small Unit Combat Simulation (DYNTACS X)--Counterbattery Fire Models," Report RF-2978-FR-70-1, Systems Research Group, Ohio State University, Columbus, OH (October 1970).

79. G. M. Clark, "Extensions to the Land Combat Model (DYNCOM). Volume 1. Helicopter and Missile Models," Report No. RF-2995-FR-71-1, Ohio State University, Systems Research Group, Columbus, OH (31 December 1971).

80. D. K. Hugus, "A Review of the Compilation of the DYNTACS(X) Data Base for the HELLFIRE COEA," Report No. CACDA-TR-9-76, Army Combined Arms Combat Developments Activity, Fort Leavenworth, KS (June 1976).

81. W. Eckhardt et al., "Air-Ground Engagement Models Review," Final Report, Office of the Assistant Vice Chief of Staff (Army), Washington, D.C. (March 1973).

82. N. D. Cohen, "An Application of Computer Graphics: The FAST-VAL Ground Unit Deployment Input System," Report No. RM-6224-PR, Rand Corp., Santa Monica, CA (April 1970).

83. S. G. Spring and S. H. Miller, "FAST-VAL: Relationships Among Casualties, Suppression, and the Performance of Company-Size Units," Report No. RM-6269-PR, Rand Corp., Santa Monica, CA (March 1970).

84. K. Harris, "FAST-VAL: Forward Air Strike Evaluation Model (Phase II Computer Program)," Report No. R-812-PR, Rand Corp., Santa Monica, CA (November 1971).

85. S. G. Spring, "Fast-VAL: A Guide for Translating a Scenario into Model Inputs," Report No. R-814-PR, Rand Corp., Santa Monica, CA (November 1971).

86. A. E. Laurence and G. V. Lucha, "FIREFIGHT 2--Users Manual," Final Report, SRI IR&D Program 30201, Task BMV, SRI International, Menlo Park, CA (June 1973).

87. H. W. Loomis, "The Fire-Fight Assessment in the Ground Combat Confrontation (Gdd) Model," Report No. NWL-TR-2156, Naval Weapons Laboratory, Dahlgren, VA (17 April 1968).

88. D. L. Smart, "Mathematical Model of Armed Helicopter vs. Tank Duel," Master's Thesis, Naval Postgraduate School, Monterey, CA (September 1972).

89. E. W. Hampton, "Infantry Combat Model," Report No. CAA-D-74-5, Army Concepts Analysis Agency, Bethesda, MD (December 1974).

90. R. D. Wollmer, "An Interdiction Model for Sparsely Traveled Networks," Report No. RM-5539-PR, Rand Corp., Santa Monica, CA (April 1968).

91. D. D. Boozer and D. Engi, "Simulation of Personnel Control Systems with the Insider Safeguards Effectiveness Model (ISEM)," Report No. SAND76-0682, Sandia Laboratories, Albuquerque, NM (April 1977).

92. D. Engi, "Nuclear Facility Safeguards Systems Modeling Using Discrete Event Simulation," Report No. CONF-770433-2, Sandia Laboratories, Albuquerque, NM (1977).

93. D. Engi and D. D. Boozer, "Use of ISEM in Studying the Impact of Guard Tactics on Facility Safeguards Systems Effectiveness," Report No. CONF-770656-21, Sandia Laboratories, Albuquerque, MN (July 1977).

94. D. D. Boozer and D. Engi, "Insider Safeguards Effectiveness Model (ISEM). User's Guide," Report No. SAND77-0043, Sandia Laboratories, Albuquerque, NM (November 1977).

95. R. W. Johnson et al., "Procedure Guide for the Individual Unit Action (IUA) Model on the Fort Leavenwortł Data Processing Installation CDC 6500 Computer System," Report No. CACDA-TR-2-73, Army Combined Arms Combat Dev Activity, Fort Leavenworth, KS (1 November 1973).

96. R. W. Johnson et al., "System Reference Manual for the Individual Unit Action (IUA) Model on the Fort Leavenworth Data Processing Installation CDC 6500 Computer System," Report No. CACDA-TR-1-73, Army Combined Arms Combat Dev Activity, Fort Leavenworth, KS (1 November 1973).

97. "Joint Limited War Counterinsurgency Operations (JOLIWACO)--Users Manual," Report No. CDC-90009-14, Control Data Corp., Honolulu, HA (21 May 1971).

98. "Joint Limited War Counterinsurgency Operations (JOLIWACO)--Analytical Manual," Report No. CDC-90009-15, Control Data Corp., Honolulu, HA (21 May 1971).

99. "Markov and Semi-Markov Modelling of Small Engagements," Report No. SANDIA-L WP77-5, Vector Research Inc., Ann Arbor, MI (20 December 1977).

100. F. K. Peterson, "A Mathematical Model of Infantry Combat," Master's Thesis, Naval Postgraduate School, Monterey, CA (April 1970).

101. L. B. Anderson et al., "An Attrition Model for Penetration Processes," Report No. P-1148, Institute for Defense Analyses, Arlington, VA (March 1976).

102. O. C. Baldonado et al., "Safeguards Systems Concepts for Nuclear Material Transportation," NUREG-0335, Final Report, Systems Development Corp., McLean, VA (September 1977).

103. O. C. Baldonado et al., "Executive Summary of Safeguards Systems Concepts for Nuclear Material Transportation," NUREG-0334, Final Report, Systems Development Corp., McLean, VA (September 1977).

104. "Modification to Math Model for Small Independent Action Forces (SIAF)," Final Report, TRW Systems Group, Redondo Beach, CA (15 December 1973).

105. "SIAF System Model User's Manual: Small Independent Action Forces. Volume II. Model Subroutines (Terrain, Weather, Targets)," Report No. 16905-6009-RD00, TRW Systems Group, Redondo Beach, CA (15 December 1973).

106. "SIAF System Model User's Manual: Small Independent Action Forces. Volume III. Model Subroutines (SIAF Functions and Ancillary Routines)," Report No. 16905-6010-RD001, TRW Systems Group, Redondo Beach, CA (15 December 1973).

107. "SIAF System Model User's Manual: Small Independent Action Forces. Volume IV. Model Program Listing," Report No. 20660-6005-RD00, TRW Systems Group, Redondo, CA (15 December 1973).

108. "SIAF System Model User's Manual: Small Independent Action Forces. Volume V. Combat Initialization Subroutines," Report No. 20660-6006-RD00, TRW Systems Group, Redondo Beach, CA (15 December 1973).

109. "SIAF System Model User's Manual: Small Independent Action Forces. Volume VI. Combat Execution Subroutines," Report No. 20660-6007-RD00, TRW Systems Group, Redondo Beach, CA (15 December 1973).

110. W. E. Deutscher, "Small Independent Action Force (SIAF), Vegetation Classification Study," Master's Thesis, Naval Postgraduate School, Monterey, CA (March 1976).

111. Myungho Oh, "Optimal Time-Sequential Distribution of Supporting Fire Against Two Enemy Ground Units," Master's Thesis, Naval Postgraduate School, Monterey, CA (September 1974).

112. E. M. Jones, "Target Acquisition Model," Report No. CAA-D-74-4, Army Concepts Analysis Agency, Bethesda, MD (December 1974).

113. R. S. Miller, "A Surveillance-Interdiction Model for Remote Area Operations," Master's Thesis, Naval Postgraduate School, Monterey, CA (March 1971).

114. T. Metkarunchit, "A Lanchester-Based Model for Investigation of Tactical Decision Rules for Two-Stage Ambushes," Master's Thesis, Naval Postgraduate School, Monterey, CA (September 1972).

115. J. J. Sternberg et al., "Selected Elements of a Battalion Integrated Sensor System: Device and Mix Effectiveness," Research Report 1183, Manned Systems Sciences Inc., Northridge, CA (January 1974).

116. R. L. Farrell, "Investigation of the Tactical Control of Cover and Exposure and Its Relation to Predicted Combat Results," Report No. VRI-DUSA-1-FR-77-1, Vector Research Inc., Ann Arbor, MI (28 February 1977).

117. J. E. Marsh, "Input Data, ARMSodel Simulation of the OH-58A in an Army Tactical Environment," Final Report No. TR-11-1, Cobro Corp., Silver Spring, MD (May 1977).

118. C. J. Needels, "The Simulation of Tactical Smoke on the Modern Battlefield," Master's Thesis, Army Command and General Staff Coll, Fort Leavenworth, KS (10 June 1977).

119. K. P. Berkbigler, "Estimating the Availability of LLEA Officers," Report No. SAND77-8626, Sandia Laboratories, Livermore, CA (July 1977).

120. J. R. Kelley, "Simulation and Analysis of Ammunition Transport Capability in Support of a Combat Unit," Master's Thesis, Naval Postgraduate School, Monterey, CA (March 1978).

121. S. C. Keeton and R. J. Gallagher, "A Tactical Game for Use in the Development and Evaluation of Road-Transit Physical Protection Systems," Report No. SAND78-8652, Sandia Laboratories, Livermore, CA (July 1978).

122. "Current Mathematical Models (for Digital Computers)," Report No. NWL-TR-2390-Rev-1, Naval Weapons Laboratory, Dahlgren, VA (August 1970).

123. W. J. Breede, III, "A Comparison of Some Lanchester Models of the Skirmish," Master's Thesis, Naval Postgraduate School, Monterey, CA (March 1971).

124. "A Hierarchy of Combat Analysis Models," General Research Corp., McLean, VA (January 1973).

125. A. R. Christensen et al., "TETAM Model Verification Study. Volume I. Representation of Intervisibility, Initial Comparisons," Report No. CACDA-TR-4-76, Army Combined Arms Combat Developments Activity, Fort Leavenworth, KS (February 1976).

126. A. R. Christensen and E. D. Arendt, "TETAM Model Verification Study. Volume II. Modified Representations of Intervisibility," Report No. CACDA-TR-5-76, Army Combined Arms Combat Developments Activity, Fort Leavenworth, KS (February 1976).

127. A. R. Christensen et al., "TETAM Model Verification Study. Volume III. Dynamic Battle Comparisons," Report No. CACDA-TR-6-76, Army Combined Arms Combat Developments Activity, Fort Leavenworth, KS (February 1976).

128. A. F. Karr, "A Class of Lanchester Attrition Processes," Report No. P-1230, Institute for Defense Analyses, Arlington, VA (December 1976).

129. D. J. Berg and M. E. Strickland, "Catalog of War Gaming and Military Simulation Models (7th Edition)," Report No. SAGA-180-77, Studies Analysis and Gaming Agency, Washington, D.C. (August 1977).

130. A. Perri, "Multisensor Target Acquisition Model Comparison," Report No. MERADCOM-2227, Army Mobility Equipment R&D Command, Fort Belvoir, VA (November 1977).

131. K. J. Murphy and K. Ikrath, "Analysis of a 'Seismic Fence' for Intrusion Detection (Experimental and Theoretical Results)," Report No. ECOM-2848, Army Electronics Command, For Monmouth, NJ (May 1967).

132. L. Berglund et al., "Field On-Line Data Acquisition and Analysis System. Concept Evaluation and System Specifications. Volume I," RADC-TR-71-103, Final Tech Report, Bunker-Ramo Corp., Westlake Village, CA (May 1971).

133. A. D. Korbut-Weberg, "Field On-Line Data Acquisition and Analysis System. Concept Evaluation and System Specifications. Volume II," RADC-TR-71-103, Final Report, Bunker-Ramo Corp., Westlake Village, CA (May 1971).

134. R. L. Allen et al., "Buried Line Sensor Evaluation for BISS. Part I. Line Sensors and Evaluation Philosophy," Report No. CONF-748427-1, Sandia Laboratories, Albuquerque, NM (1974).

135. R. L. Allen et al., "Buried Line Sensor Evaluation for BISS. Part II. Evaluation Results," Report No. CONF-758514-1, Sandia Laboratories, Albuquerque, NM (1975).

136. D. W. Wall et al., "Programmer's Description of the Barrier Data Base," SAND76-0522, Sandia Laboratories, Albuquerque, NM (December 1976).

137. P. B. Scott, "Voice Input Code Identifier (VICI),' RADC-TR-77-190, Final Tech Report, Threshold Technology Inc., Delern, NJ (June 1977).

138. N. R. Wagner, "A Survey of Threat Studies Related to the Nuclear Power Industry," Report No. SAND77-8254, Sandia Laboratories, Albuquerque, NM (August 1977).

139. A. M. Fine, "Physical Attributes of Potential Adversaries to U.S. Nuclear Programs," Report No. CONF-770320-1, Sandia Laboratories, Albuquerque, NM (1977).

140. S. Scala, "Generic Data Base for Modeling Safeguards Security Equipment, Volume 1 of Part 1: Discussion," Report SRI Project 6220, SRI International, Menlo Park, CA (September 1977).

141. A. Fainberg and A. M. Bieber, Jr., "Barrier Penetration Data Base," PB-283 046, Brookhaven National Laboratory, Upton, NY (July 1978).

142. A. W. Wiegand et al., "Generic Data Base for Modeling Safeguards Security Equipment, Annex to Volume 1," Report SRI Project 6220, SRI International, Menlo Park, CA (August 1978).

143. "Systems Analysis Directorate Activities Summary, May 1976," Report No. DRSAR/SA/N-47, Army Armament Command, Rock Island, IL (June 1976).

144. D. D. Boozer et al., "Safeguards System Effectiveness Modeling, Report No. CONF-760615-14, Sandia Laboratories, Albuquerque, NM (September 1976).

145. L. D. Chapman, "Physical Protection of Nuclear Facilities," SAND77-0487, Quarterly Progress Report, October-December 1976, Sandia Laboratories, Albuquerque, NM (April 1977).

146. R. L. Rinne, "Evaluation of Safeguards Systems for Nuclear Material in Transit: The Development of the Program Plan," SAND77-8249, Winter 1977 Quarterly Report, Sandia Laboratories, Livermore, CA (July 1977).

147. V. L. Dugan and L. D. Chapman, "A Structure for the Decomposition of Safeguards Responsibilities," Report No. SAND77-0400, Sandia Laboratories, Albuquerque, NM (August 1977).

148. L. D. Chapman, "Physical Protection of Nuclear Facilities," SAND77-1622, Quarterly Progress Report, April-June 1977, Sandia Laboratories, Albuquerque, NM (October 1977).

149. L. D. Chapman, "Physical Protection of Nuclear Facilities," SAND77-2107, Quarterly Progress Report, July-September 1977, Sandia Laboratories, Albuquerque, NM (March 1978).

150. "A Systematical Approach to the Conceptual Design of Physical Protection Systems for Nuclear Facilities," Report HCP/D0789-01, Sandia Laboratories, Albuquerque, NM (May 1978).

151. "DOE Assessment Guide for Safeguards and Security," PNL-2576, Battelle, Pacific Northwest Laboratories, Richland, WA (May 1078).

152. L. D. Chapman, "Physical Protection of Nuclear Facilities," SAND78-0730, Quarterly Progress Report, October-December 1977, Sandia Laboratories, Albuquerque, NM (June 1978).

153. L. D. Chapman,et al., "Safeguards Automated Facility Evaluation (SAFE) Methodology," Report No. SAND78-0378, Sandia Laboratories, Albuquerque, NM (August 1978).

# Appendix

# SIMULATION SUMMARIES

This appendix presents summary descriptions of the simulations that were assessed during the course of this research. The numbering of the simulations in this appendix is in accordance with their respective numbering in Table 5.1 of the main text. The summary descriptions are extracted, where possible, from one of the cited references for that respective simulation. In certain cases where a simulation or simulation concept is not given a short title or acronym, we have introduced a short descriptive title for convenience.

# Appendix

# SIMULATION SUMMARIES

1. SIMULATION: Armed Escort Model

DEVELOPING AGENCY: Electronic Associates, Inc.

REPORT REFERENCE NO: 25,26

DESCRIPTION: The Armed Escort Model is a set of digital computer programs written to simula*e an engagement between a single ground weapon and a formation of troop-carrying helicopters (UH-1) escorted by a single armed aircraft. The model was constructed for the purpose of evaluating the effectiveness of different escort aircraft along various maneuvers, armed with different weapon systems, and provided data for use in a comparison study. A dual-purpose digital simulation program was written to evaluate the outcome of a single engagement in terms of expected numbers of aircraft lost, probabilities of specific damage inflicted, and similar results. The first objective was to provide a model to be used in studying the outcome of an engagement between the single ground weapon and an unescorted formation of lift aircraft that first approach the weapon position, hover for several seconds to unload or take on troops, and then pull out along the prescribed flight path. The second objective was to provide a computer model to evaluate the outcome of a similar engagement including an armed escort aircraft.

2. SIMULATION: EASI

DEVELOPING AGENCY: Sandia Laboratories

REPORT REFERENCE NO: 27-30

DESCRIPTION: A simple, easy-to-use method, called Estimate of Adversary Sequence Interruption (EASI), has been developed to evaluate physical security system performance under specified conditions of threat and system operation. The method consists of a probabilistic analysis of the interactions of basic security functions, such as detection, communications, response, etc. The evaluation can be performed on a hand-held programmable calculator. The results of the analysis are expressed in terms of the probability that the physical protection system can respond in time to interrupt specific adversary action sequences. The utility of the method depends upon the user's ability to identify significant adversary action sequences and to obtain data that properly reflect conditions created by the adversary action sequence of interest.

3. SIMULATION: FESEM

DEVELOPING AGENCY: Sandia Laboratories

REPORT REFERENCE NO: 31-33

DESCRIPTION: The Forcible Entry Safeguards Effectiveness Model (FESEM) is a combined (discrete and continuous) computer model for analyzing fixed-site security systems as to their effectiveness against a forcible entry, for any assumed physical path, by an adversary having a variety of attributes and gives an estimate of adversary success probability. The model includes variables related to detection, assessment, communication, delay, and neutralization. Output statistics on various aspects of each scenario are prcvided by the model and may be utilized by the decision maker as an aid in evaluating or upgrading a physical protection system.

4. SIMULATION: Pathfinding Codes

DEVELOPING AGENCY: Sandia Laboratories

REPORT REFERENCE No: 34-39

DESCRIPTION: The Pathfinding Codes denoted here represent a set of computer codes developed to establish optimum paths for adversaries to follow in covert sabotage, control, or theft attempts against fixed nuclear sites. The sites are defined by a graph of nodes and connecting arcs. Each node and connecting arc is provided a weight factor. The weight factor can be the expected adversary traversal time through a node or over an arc; it can be the probability of detection while traversing through a node or over an arc; ot it can be both.

The computer codes are designed to determine the optimum path for an adversary, where in one case the optimization is in terms of minimizing the adversary's time to reach his goal (and escape in the theft case) and in another case the objective is to minimize the probability of detection. A combined case considers a locus of nodes that are no more than a security force's response time away from the goal node. The algorithm then selects the optimum path by minimizing the detection probability into this locus of nodes and then minimizing the traversal time to the goal node.

5. SIMULATION: PENAIR

DEVELOPING AGENCY: Naval Postgraduate School

REPORT REFERENCE NO: 40

DESCRIPTION: PENAIR is a time-step computer simulation of an aircraft flight over hostile terrain. It is an analytic computer war game in which one aircraft and a maximum of 200 weapons are the principals. Any piece of actual terrain may be simulated using a contour map of the area to obtain the input parameters. The simulation is intended as a tool for the determination of appropriate defensive tactics for an aircraft upon receiving fire from conventional ground weapons. Using the characteristics of the aircraft and of the weapons the model determines the survival probability of the aircraft on any of several flightpaths. There are no restrictions on the aircraft's speed, altitude, or other characteristics and therefore this model is equally suitable for helicopters or jets. The aircraft flight path can be predetermined or it can be generated by the model. Upon receiving fire the aircraft can be programmed to execute any of 18 evasive maneuvers. A comparison of the survival probabilities can then be made, thus giving an indication of the appropriate defensive maneuver to employ.

6. SIMULATION: SABRES

DEVELOPING AGENCY: Sandia Laboratories

REPORT REFERENCE NO: 41-43

DESCRIPTION: The SABRES code is a time-stepped Monte Carlo simulation developed to evaluate the outcomes of engagements between attackers and defenders after a transport vehicle has been stopped. At every time step, detection, posture, firing allocation, casualty assessment, suppression, and disengagement are considered for each participant, and the results are catalogued before moving to the next time step. The battle terminates when one side disengages. The program outputs for a series of replications of an ambush are the expected survivors on each side, the fraction of time each side is totally successful, and the expected battle time.

7. SIMULATION: Schaffer's Ambush Model

DEVELOPING AGENCY: Naval Postgraduate School

REPORT REFERENCE No: 44

DESCRIPTION: The Schaffer Ambush model is a mixed Lanchester linear/square-law attrition simulation that is representative of the many Lanchester-type simulations that could be used to evaluate the outcomes of transport vehicle ambushes. The simulation assumes that an ambusher force is in concealed positions and initiates a surprise attack when the ambushee force arrives in a "killing zone." The ambushers' initial fire is aimed (Lanchester square law) while the ambushees initially react with area fire (Lanchester linear law). As the ambushees locate cover and begin to detect ambusher fire locations, they gradually switch from area to aimed fire. The ambushers maintain aimed fire throughout the engagement, although its effectiveness decreases as the engagement progresses. Ambushee desertions and ambusher withdrawals are considered in the simulation and supporting weapons for the ambusher can also be included. For the initial surprise attack, the use of claymores is also an option.

8. SIMULATION: SOURCE

DEVELOPING AGENCY: Sandia Laboratories

REPORT REFERENCE NO: 42,43,45

DESCRIPTION: SOURCE is a computer code that has been developed to study the impact of convoy configuration and tactics upon personnel survival and emergency signal generation during an initial armed attack. The SOURCE code is a flexible, time-stepped Monte Carlo model that provides for extensive variations in convoy configuration (number of vehicles, distributions, vulnerabilities, velocity, and communications) and in adversary characterization (number of units, deployment, and weapon capabilities). In the SOURCE code, the convoy is described by the number of vehicles and their positions, vulnerable areas, observation conditions, and communications capabilities. Convoys consisting of a number of different types of vehicles can be studied. Emergency messages can also be initiated, either by a vehicle under attack or by one vehicle that has observed an attack on another. The conditions under which an attack is observed can be varied, and the capability of sending a message depends on the condition of the convoy crew and their equipment. SOURCE calculates the damage to personnel and equipment and includes the cumulative effects of multiple hits.

9. SIMULATION: TSEM

DEVELOPING AGENCY: The BDM Corporation

REPORT REFERENCE NO: 46-48

DESCRIPTION: The TSEM (Transportation Safeguards Effectiveness Model) is designed to simulate a two-sided engagement between a group of adversaries and a road convoy. TSEM is a discrete, stochastic event-driven simulation that individually models persons (with their associated weapons) and vehicles. The players in TSEM (i.e., persons and vehicles) can be directed by a script that includes actions (movement, firing, and dismounting) and contingency situations (player or vehicle at a location, players dead, attack started). The battles take place on a two-dimensional surface with terrain and vegetation superimposed. The line-of-sight interruptions due to vehicles and terrain and vegetation features are correctly calculated and taken into account in firing allocation. The battles progress until all people on one side are killed off, a preset time limit is reached, or prime vehicle penetration is successfully completed. A movie can be produced that shows the course of battle, including player movements and shots fired.

10. SIMULATION: VISA

DEVELOPING AGENCY: Science Applications, Inc.

REPORT REFERENCE NO: 49,50

DESCRIPTION: Vulnerability of Integrated Safeguards Analysis (VISA) is an evaluation method that can be used to evaluate the effectiveness of fixed-site security systems against hostile encounters, both overt and covert. The method is divided into three sections: preparation, analysis, and assessment. The preparation section is simply a formalization of the site data input preparation process, and the assessment section is essentially concerned with the storage of case analysis results, with procedures to assess these results at different levels of detail via an interactive display terminal. The analysis section, which includes the principal evaluation tools, consists of four analysis modules (Path, Detection, Containment, and Interruption) and requires two data bases (Detection Mechanism, and Delay Mechanism and Engagement). Included in the Containment Analysis Module is a detailed network simulation that includes aggregated delay time and engagement simulations to evaluate the probabilities of adversary success along AAS segments.

11. SIMULATION: Adversary Action Modeling

DEVELOPING AGENCY: Lawrence Livermore Laboratory

REPORT REFERENCE NO: 51-53

DESCRIPTION: An assessment procedure has been developed to evaluate the effectiveness of a potential nuclear licensee's material control system. The first step in this procedure is to identify targets within the facility that contain theft-attractive special nuclear material. The second step is to determine the adversary actions and conditions of the material control system that could allow successful diversion of special nuclear material--that is, generate the adversary event sets. Simulation is required for adversary event sets where timeliness and ordering of events is important for successful diversion. The qualitative and quantitative analysis of the event sets and the simulation results allow the effectiveness of the material control system to be determined.

12. SIMULATION: AIDM Supression Model

DEVELOPING AGENCY: BDM Services Company

REPORT REFERENCE NO: 54

DESCRIPTION: A suppression model has been developed for inclusion in the AMSAA Improved Differential Model (AIDM). The model includes suppression of and by every weapon group to be played with the exception of an AH (attack helicopter) group suppressing an AH group. Suppression is represented via a two-state Markov chain model in which a weapon is either in the suppressed or unsuppressed state, with the transition to the next state depending only on the current state and not on the past history of the weapon's suppression. The model requires the probabilities of changing states in the time interval, $\Delta t$. This probability is calculated as a function of the numbers of rounds of all types directed at the weapon during the interval.

13. SIMULATION: AIRCAV

DEVELOPING AGENCY: Vector Research, Inc.

REPORT REFERENCE NO: 55,56

DESCRIPTION: AIRCAV is a set of two differential model programs incorporating AH and ADW activities, differing principally in the detailed assumptions and logic of their ground scenarios and the format of their data bases. Both models treat a battalion-level engagement between Red and Blue forces, with Blue forces including attack helicopters (AHs) in direct support and Red forces including air defense weapons (ADWs). These programs were constructed as modifications of existing differential model programs treating ground combat without AH support. The scenarios were therefore constructed as modifications of basic ground combat scenarios.

14. SIMULATION: AMSWAG

DEVELOPING AGENCY: Army Material Systems Analysis Agency

REPORT REFERENCE NO: 57

DESCRIPTION: The AMSAA War Game (AMSWAG) model is a time sequenced, deterministic, battalion-level, force-on-force computer model that simulates a classical attack and defense. Up to 64 defenders are deployed in fixed positions in hull defilade. The attacking force has already deployed and moves along predetermined routes of advance toward the defender. The attacking force is allowed a maximum of 12 routes of approach. The routes are administratively broken into one to three groupings of up to four routes each. These groupings are called axes, and each axes nominally contains a company-sized force. Thus, each route nominally contains a platoon. This platoon can be further split into two homogeneous sections (of two to four vehicles each) that maneuver together down the route. Normal movement techniques for these sections are either alternate bounds or successive bounds. The model conducts the battle in uniform time steps of 10 seconds each.

15. SIMULATION: Analytic Engagement Model

DEVELOPING AGENCY: Sandia Laboratories

REPORT REFERENCE NO: 58

DESCRIPTION: The Analytic Engagement Model is a discrete-state, continuous-time stochastic process. The state of the battle is described simply in terms of the number of guards and adversaries actively engaged in battle, along with the number of arrivals of friendlies to each of the opposing forces. The solution procedure is analytical in nature and involves solving sets of linear equations. For small battles, consisting of one or two combatants on each side, symbolic solutions can be found. If the input parameters are not all distinct, it may be feasible to obtain symbolic solutions for larger battles. The procedure can be used to compute analytic numerical solutions for larger battles with a total of less than 10 combatants on both sides.

16. SIMULATION: ARMREC

DEVELOPING AGENCY: Naval Postgraduate School

REPORT REFERENCE NO: 59

DESCRIPTION: ARMREC is a time-step computer simulation of an armed reconnaissance flight of two helicopter sections in search of a small stationary or moving armored land target. Simultaneous and independent movement of the participants is provided for in the model, and all movement takes place over terrain simulated by a "least-squares" polynomial. The necessary data for the terrain simulation in ARMREC is supplied by a separate program, TERRAIN. The flight paths of the helicopter sections in the model are either preplanned, and as such are included with the necessary input data for the model, or they are generated as nap-of-the-earth (NOE) flight paths by the ARMREC program.

17. SIMULATION: Bonder/IUA

DEVELOPING AGENCY: Army Material Systems Analysis Agency

REPORT REFERENCE NO: 60

DESCRIPTION: The Bonder/IUA model is an adaptation of the general Bonder methodology to the Individual Unit Action (IUA) simulation scenarios. The Bonder model is a generalized differential equation model of ground combat. It is an extension of the Lanchester analytic formulations. In contrast to the classical Lanchester approach, which based attrition rates on historical data, this model estimates attrition rates based on measurable weapon system parameters. It also allows playing of heterogeneous forces. Weapons of a given type in the same general location are aggregated into a single group. Different types of weapons and weapons of the same type in different locations are played as distinct groups.

18. SIMULATION: Breakpoints in Land Combat

DEVELOPING AGENCY: Naval Postgraduate School

REPORT REFERENCE NO: 61

DESCRIPTION: This concept considers battle termination (a unit reaching its so-called "breakpoint") in ground combat as a rational decision process. A commander's decision to break contact with an enemy force and withdraw from the battlefield is analyzed for company-size infantry units. Two approaches for modeling a commander's decision process to terminate an engagement are presented. The first approach is based on extrapolation of observations on past battle history into the future with no assumption about combat dynamics. The second is based on the assumption of known Lanchester-type combat dynamics (possibly with unknown parameters to be estimated) and uses Kalman filtering.

19. SIMULATION: Brookhaven PPM

DEVELOPING AGENCY: Brookhaven National Laboratory

REPORT REFERENCE NO: 62

DESCRIPTION: The Brookhaven Physical Protection Model (also called PROTMOD) is a computer simulation used to evaluate physical protection of fixed sites. The model computes the outcome of an input adversary action sequence. The result is deterministic in that all variables and parameters are fixed for a given case. That is, there are no probabilistic considerations. This is an interactive model, designed to be run from the facility via a remote data terminal. The model prompts the user for all required input and prints all output at the remote terminal.

20. SIMULATION: CARMONETTE

DEVELOPING AGENCY: General Research Corporation

REPORT REFERENCE NO: 60,63-71

DESCRIPTION: CARMONETTE is a critical-event-sequenced infantry combat simulation of the activities of movement, target acquisition, communications, and weapon employment. When a unit comes within line of sight of an enemy unit, it has a probability of acquiring information about the enemy as a target. The information it may acquire ranges from none to full knowledge of the exact location and nature of the enemy unit. If the unit gets sufficient information and has an appropriate order, it will select weapons and ammunition and take the enemy under fire. A weapon is simulated in terms of its rate of fire and its maximum range. The effects of a projectile are simulated by tables giving the probabilities that it will hit what it was aimed at as a function of the range and the size of the target, and by further tables giving the probability that it will kill the target if it hits it. Explosive projectiles are characterized in terms described on the basis of their average rates of movement under various conditions and in terms of their vulnerability to different kinds of weapons. Aircraft are characterized by their vertical and horizontal components of velocity and their vulnerability. Firing may be terminated by lack of ammunition, loss of target information, death of the firing unit, known death of the target unit, or expenditure of an ordered amount of ammunition or time.

21. SIMULATION: Countermeasures Engagement Analysis

DEVELOPING AGENCY: Air Force Institute of Technology

REPORT REFERENCE NO: 72

DESCRIPTION: This analysis involved the construction of a computer model to study a one-on-one engagement. It is built so that parameters in the RF or optical regime can be used. The aircraft flies over the threat, is not allowed to maneuver, and the atmosphere has been ignored.

Fly By 1 introduces the techniques employed by the GASP IV simulation language. The aircraft is detected when it comes within range. In Fly By 2, a more probabilistic determination of detection is used, and the radar scans for the aircraft. Fly By 3 makes 20 runs of the Fly By 2 program and collects statistics on the range of detection. Fly By 4 incorporates a track-and-fire role into the threat.

22. SIMULATION: Daylight Assault Model

DEVELOPING AGENCY: Naval Postgraduate School

REPORT REFERENCE NO: 73

DESCRIPTION: With Lanchester's Square Law providing a point of departure, a model of small-unit combat was developed in which major parameters of an encounter known to be time- or range-dependent were so treated, thus incorporating realism of dynamic combat. The single uncontrolled variable of the model is force size. Force sizes were specified at the start of each computer battle simulation; however these sizes were updated by the computer program every one-tenth of a minute of the battle. The remaining variables were controlled in that they were either assumed, calculated from other data, or direct input values from other research. Success in battle was considered dependent upon infliction of casualties on the opposing force and the range between the forces at the termination of the engagement.

23. SIMULATION: DYNTACS

DEVELOPING AGENCY: Ohio State University

REPORT REFERENCE NO: 60,74-80

DESCRIPTION: DYNTACS is a small-unit, high-resolution simulation that can represent combat engagements ranging in size from a single element to a reinforced armored battalion. The attack, defense, delay, and meeting engagements can be portrayed. Armor, artillery, air defense, attack helicopters, crew-served weapons, and mounted infantry in the attack are modeled. Dismounted infantry cannot be played; the smallest resolution is the individual vehicle. Combat is represented as an adaptive process where each unit is constantly evaluating the battle situation in order to pick the tactic most appropriate for the tactical doctrine expressed by the input data.

24. SIMULATION: EVADE

DEVELOPING AGENCY: Army Materiel Systems Analysis Agency

REPORT REFERENCE NO: 81

DESCRIPTION: EVADE is a deterministic computer simulation developed to evaluate the attrition of both air and ground participants as multiple aircraft fly missions over deployments of air defense weapons. Extensive use is made of digitized descriptions of terrain maps with superimposed vegetation. Great detail is possible in the aircraft vulnerability portion of EVADE, with components (engine, pilot, hydraulics, etc.) treated separately, if desired, and with vulnerable areas being varied according to the aspect angle from the weapon site. Appropriate combination of all of the component damage probabilities can then yield aircraft attrition probabilities in several categories, such as crash, forced landing, and abort. The time history of probability of kill for each element in the simulation is made available to the user of EVADE. The model is useful as a relative survivability indicator for obtaining a first-order estimate of the practicality or adequacy ι_ flight paths, weapon deployments, tactics, equipment, etc.

25. SIMULATION: FAST-VAL

DEVELOPING AGENCY: Rand Corporation

REPORT REFERENCE NO: 82-85

DESCRIPTION: FAST-VAL is a simulation model developed to investigate the value of airpower in support of ground combat. To this end, the model is structured to provide a framework in which a wide range of ground engagements, company through regimental size, can be simulated while maintaining the level of detail necessary to evaluate the influence of different air and ground weapon systems upon the outcome of the engagements. In a simulation, two deployed forces exchange mortar fire, artillery fire, and air strikes. Attacking rifle companies advance and exchange rifle and machinegun fire with defending rifle companies. A set of decision rules relates the influence of supporting weapons fire and small-arms fire to the behavior of the engaged infantry companies and the outcome of the engagement. The inclusion of the interaction of infantry units allows the value of the supporting fire to be measured in terms of both the engagement outcome and the expected casualties. The model is structured so that engagements can be simulated without supporting fire, and then resimulated with varying amounts of supporting fire, with the timing and targeting of supporting fire controlled by the model user.

26. SIMULATION: FIREFIGHT

DEVELOPING AGENCY: SRI International

REPORT REFERENCE NO: 86

DESCRIPTION: FIREFIGHT is a computer simulation developed to evaluate the effectiveness of alternative small arms, using the criterion of tactical mission success probability. It can be used to evaluate rifles, machineguns, grenade launchers, and grenades. Mortar, artillery, and other supporting fires are not explicitly modeled. This small-unit simulation can also be used to study tactics or nonweapon equipment options.

27. SIMULATION: GCC Firefight

DEVELOPING AGENCY: Naval Weapons Laboratory

REPORT REFERENCE NO: 87

DESCRIPTION: The Firefight Submodel of the Ground Combat Confrontation (GCC) is a tool of military operations analysis designed to assess the results of close combat between opposing forces of mixed infantry and mechanized units. The forces are considered to be composed of "fire units," such as a USMC fire team or a single tank, elements of the forces that have their target acquisition, fire, and movement internally coordinated. Detailed round-by-round assessments are given to the fire of individual crew-served tank and antitank weapons possessed by a fire unit. The lethal and suppressive effects of individual projectiles are considered in terms of the activity and presentation of the target fire unit.

28. SIMULATION: Helicopter vs. Tank Duel

DEVELOPING AGENCY: Naval Postgraduate School

REPORT REFERENCE NO: 88

DESCRIPTION: The purpose of this concept is to mathematically model a duel between an armed helicopter and a tank. In addition to providing a parametric analysis of B. O. Koopman's classical Detection-Destruction Duel, two additional models were constructed and analyzed. All three models stem from stochastic versions of Lanchester's equations, but require that a unit first be detected before it is destroyed. The later two models are extensions of Koopman's model but provide for the unique capability of the helicopter to rapidly maneuver behind masking terrain, thus transitioning from the detected state back to the undetected state. With further refinement, these models may prove to be a viable alternative to the current method of computer simulation.

29. SIMULATION: ICM

DEVELOPING AGENCY: Army Concepts Analysis Agency

REPORT REFERENCE NO: 89

DESCRIPTION: The Infantry Combat Model (ICM) is a two-sided ground combat model (designed for computer use) that simulates small infantry unit engagements of close combat over successive finite time intervals. The units can contain varying numbers of personnel with a variety of direct-fire weapons. Each unit can be augmented by reserve forces and can be supported by indirect fire of varying types. Each engagement is evaluated on the basis of assessing personnel casualties and ammunition expenditures in successive finite time intervals. The results are accumulated until the exchange terminates based on predetermined conditions. Each engagement is replicated and the results are averaged. The model output consists of average personnel casualties for both sides, direct- and indirect-fire weapon ammunition expenditures, termination distances between opposing forces, direct-fire weapon attrition, and average engagement time.

30. SIMULATION: Interdiction Model

DEVELOPING AGENCY: Rand Corporation

REPORT REFERENCE NO: 90

DESCRIPTION: The Interdiction Model is an algorithm for determining where to place forces in order to maximize the probability of preventing an opposing force from proceeding from one particular node in a network to another.

The usual gaming assumptions are invoked in this model--namely, that the strategy for placing forces is known to the opponent and that he will choose a path through the network that, based on this knowledge, maximizes his probability of successful traverse. As given quantities, the model requires a list of the arcs and nodes of the network, the number of forces available to stop the opposing force, and the probabilities for stopping the opposition at the arcs and nodes as functions of the number of forces placed there. From these data, the model calculates the probabilities for placing the force at the arcs and nodes when one force is available, and the expected numbers of forces to place at the arcs and nodes when multiple forces are available.

31. SIMULATION: ISEM

DEVELOPING AGENCY: Sandia Laboratories

REPORT REFERENCE NO: 91-94

DESCRIPTION: The Insider Safeguards Effectiveness Model (ISEM) is a model used to evaluate facility safeguards system effectiveness for threats posed by insiders. The general safeguards problem posed by the insider threat requires consideration of material control, material accounting, and personnel control systems. ISEM was developed to treat specifically those insider attacks in which the time relationship among scenario events is important. The concept of attack detection leading to a safeguards system response is central to the model. The set of scenario events for one attack may include events from the material control, material accounting, and personnel control systems; however, there is no distinction made between these major safeguards subsystems within the model. An important class of insider scenarios treated by ISEM is one in which some response by security guards is required to prevent the successful completion of the insiders' attack. ISEM can model either theft or sabotage attacks that consist of both nonforcible and forcible adversary actions. Among the effectiveness measures that can be obtained from ISEM are estimates of (1) the probability of at least one alarm along the adversary path, (2) the probability of at least one encounter between the adversary and response guards along the adversary path, and (3) the probability that the adversary is thwarted along the adversary path either by encounters with guards or by being caught in portals.

32. SIMULATION: IUA

DEVELOPING AGENCY: Combined Arms Combat Development Activity

REPORT REFERENCE NO: 60,95,96

DESCRIPTION: The Individual Unit Action (IUA) is a computerized simulation of a mall-unit (company/battalion size) tank-antitank battle to evaluate combat effectiveness of candidate tank and antitank weapon systems, and to evaluate the relative combat effectiveness of alternative mixes of tank and antitank weapons. The simulation plays the interaction of various weapon systems including tank, antitank weapons, armored personnel carriers, artillery, mines, helicopter-borne weapons, and tactical close-support aircraft. The primary focus of IUA is on tank and antitank systems; other weapon systems effects are played with minimum detail compared to tank and antitank systems.

The structure of the simulation is "event-oriented," which means that time is not handled at uniform intervals. An executive routine determines the order in which events are processed and maintains a continually updated table that indicates the chronological order of events to be processed.

The submodels may be divided into two classes by techniques employed--deterministic, and stochastic. The terrain and mobility submodels are deterministic. The acquisition and weapons-effects submodels are stohastic. The target allocation model uses a set of priorities based on user input.

33. SIMULATION: JOLIWACO

DEVELOPING AGENCY: Control Data Corporation

REPORT REFERENCE NO: 97,98

DESCRIPTION: Joint Limited War Counterinsurgency Operations (JOLIWACO) is a computer-assisted manual war game between an insurgent force and a counterinsurgent force. An indigenous population also is assumed with the ability to provide intelligence, manpower, and supplies to either side. Depending on the scenario, any level of operations (village to national) may be modeled. Human players determine mission and policy. Lanchester-type models are used to determine outcomes of intelligence missions, engagements, and so on. Game outputs include resources consumed, casualties suffered, and mission results for the two forces and the indigenous population.

34. SIMULATION: Markov Engagement Model

DEVELOPING AGENCY: Vector Research, Inc.

REPORT REFERENCE NO: 99

DESCRIPTION: The Markov Engagement Model is a conceptual formulization of a Markov or Semi-Markov model to evaluate the outcome between a set of attackers and a guard force. The range between opposing participants is approximately constant. The model allows for the possibility of arriving forces joining one side or both. The model does not allow for range closure, changes in force posture, exhaustion of ammunition supplies, and so on. However, modifications of the process are suggested to overcome some of the restrictions.

35. SIMULATION: Math Model of Infantry Combat

DEVELOPING AGENCY: Naval Postgraduate School

REPORT REFERENCE NO: 100

DESCRIPTION: This is a deterministic mathematical model of combat that takes into account the phenomenon of fire suppression. This model, based on Lanchester's theories of combat, can be used to investigate the offensive tactics and defensive fire distribution of a small-scale infantry action. Specifically, the type of action covered is an attack against a defended position. The missions of the attacking and defending units are, respectively, to gain or maintain control of the defended position while holding their own casualties to a minimum. The offensive force has two tactics it can employ--advance its entire force against the enemy, or advance only a portion of its force while using the remainder to lay down a covering fire. The defense then has the decision of how to divide its fires to engage the attacking elements.

36. SIMULATION: Penetration Attrition Model

DEVELOPING AGENCY: Institute for Defense Analyses

REPORT REFERENCE NO: 101

DESCRIPTION: The Penetration Attrition Model is a probabilistic model designed to evaluate the combat attrition between attackers (infiltrators) and defenders attempting to defend a passive target. Infiltrators attempt to reach a target successively, one after another. An infiltrator is detected by each defender present with a constant probability, independent of any other defender and of past history. When a detection occurs, exactly one defender is assigned to engage the infiltrator. One-on-one engagements are evaluated by assigning probabilities, independent of past history, to the possible outcomes. Probability distributions are computed for infiltrators destroyed, infiltrators reaching target, and defenders destroyed, all conditioned on K attempted penetrations.

37. SIMULATION: SDC Transportation Model

DEVELOPING AGENCY: Systems Development Corporation

REPORT REFERENCE NO: 102,103

DESCRIPTION: The SDC Transportation Model is a methodology that includes techniques for defining, classifying, and analyzing adversary action sequences; defining safeguards system components; assessing the vulnerability of various safeguards systems and their component parts to the potential adversary action sequences, and conceptualizing system design requirements. The method of analysis is based primarily on a comparison of adversary actions with safeguards measures to estimate vulnerability. Because of the paucity of the data available for assessing vulnerability, the Delphi approach is used to generate data; values are estimated in a structured exercise by a panel of experts in the safeguards and terrorist fields.

38. SIMULATION: SIAF

DEVELOPING AGENCY: TRW Systems Group

REPORT REFERENCE NO: 62,104-110

DESCRIPTION: The Small Independent Action Force (SIAF) computer model has been developed to analyze the effectiveness of small patrols. In the model, patrols of up to 20 men can cover an area about 25 $km^2$. The model simulates the detection and engagement of enemy units involving less than 20 men or positions. The model can accommodate a time period of up to 10 days. A combination of graph ("grid") and event-driven techniques is used for the simulation. Submodels include enemy situation, command and control, communications, human maintenance, supply maintenance, fire support, surveillance/detection, navigation, movement, terrain, and weather. Output consists of an event table providing what happened at what time. This model may contain submodels useful in enhancing the capabilities of the physical protection model. The SIAF model avoids the use of force engagement models such as the Lanchester relations by keeping track of the performance and vulnerability of each combatant.

39. SIMULATION: Supporting Fire Model

DEVELOPING AGENCY: Naval Postgraduate School

REPORT REFERENCE NO: 111

DESCRIPTION: The optimal time-sequential distribution of supporting fire against enemy ground units in combat against attacking friendly units is studied. Lanchester-type models of warfare are combined with optimal control theory in this investigation. The optimal time-sequential fire-support policy is characterized for a specific problem. Although complete details for the determination of the optimal policy are not given, it is conjectured, on the basis of the theorems that were proved, that for this problem the optimal policy is to always concentrate all supporting fire on the same enemy unit (until supporting fire must be lifted).

40. SIMULATION: TAM

DEVELOPING AGENCY: Army Concepts Analysis Agency

REPORT REFERENCE NO: 112

DESCRIPTION: The Target Acquisition Model (TAM) is a simulation of the acquisition of targets in a target force by the sensors of an acquiring force. The purpose of the simulation is the generation of acquisition events that will ultimately result in requests for fire missions to be delivered by an artillery firing force. The target force, represented to the model by a static target array, is played at the small-unit level of resolution. The acquiring force is played at the individual-sensor level of resolution. The model addresses input target arrays for a 6-hour game time period and produces an a-priori list or history of acquisition events.

41. SIMULATION: TRW PPM

DEVELOPING AGENCY: TRW Systems Group

REPORT REFERENCE NO: 62

DESCRIPTION: The TRW Physical Protection Model (PPM) is a computer program to evaluate safeguards at a fixed site against a threat of a single unit consisting of any number of persons acting together to remove special nulcear material. The assault team can consist of insiders or outsiders (but not both) in any single pass through the technique and can employ either force or stealth to gain access to a protected area or vault. Only physical security systems are modeled. The technique uses graph techniques ("grid points") and has been demonstrated for two "real world" cases of physical security at commercial buildings. (The results are classified and unavailable for this report.) Route optimization, which considers all possible geometric paths, is achieved via "forward dynamic programming." The overall probability of mission success is optimized. An effort is made to characterize a facility "realistically" in terms of walls, doors, locks, and other familiar items. The progress of the attack is monitored from grid point to grid point. Sensors including fixed electronic sensors and roving patrols provide the start signal for the guard forces to respond. The response and time of arrival of the guard force depend on their posture, procedures, and the characteristics of the facility. The model terminates the adversary action sequence with the arrival at the protected area of the attackers or the security force. A mob action model simulating the interaction of mobs with security guards is included in the program. This and a bomb damage model are used in a stand-alone mode. The final result is the probability that the adversary can access a restricted area and depart via the optimum path before the guard force arrives.

# DISTRIBUTION LIST

## DEPARTMENT OF DEFENSE

U.S. Documents Officer, AFSOUTH
ATTN: U.S. Documents Officer

Armed Forces Staff College
ATTN: Reference & Technical Services Branch

Assistant Secretary of Defense
International Security Affairs
ATTN: Policy Plans & NSC Affairs
ATTN: NATO Nuclear Policy Div.
ATTN: P & P Nuclear Policy
ATTN: European & NATO Affairs

Assistant Secretary of Defense
Comm., Cmd., Cont., & Intell
ATTN: Surveillance & Warning System
ATTN: Combat Support
ATTN: Intelligence Systems

Assistant Secretary of Defense
Program Analysis & Evaluation
ATTN: General Purpose Programs
ATTN: Strategic Programs
ATTN: Regional Programs

Assistant to the Secretary of Defense
Atomic Energy
ATTN: Executive Assistant

Command & Control Technical Center
ATTN: Director

Commander-in-Chief
U.S. European Command
ATTN: J-3
ATTN: J-2
ATTN: J-5NPG
ATTN: J-2-ITD
ATTN: J-5
ATTN: J-417-LW
ATTN: J-6

Commander-in-Chief, Pacific
ATTN: J-3
ATTN: J-54
ATTN: J-6
ATTN: J-2

Defense Advanced Rsch. Proj. Agency
ATTN: TTO

Defense Communications Agency
ATTN: Director

Defense Communications Engineer Center
ATTN: Director

Defense Intelligence Agency
ATTN: DT-1
ATTN: RDS-3C

Defense Nuclear Agency
ATTN: DDST
ATTN: OASO
ATTN: STSS
4 cy ATTN: TITL

## DEPARTMENT OF DEFENSE (Continued)

Field Command
Defense Nuclear Agency
ATTN: FCC-FCRRK
ATTN: FCP-FCRRA
ATTN: FCP-FCPRT

Field Command
Defense Nuclear Agency
Livermore Division
ATTN: FCPRL

Intelligence Center, Pacific
ATTN: I-3

Interservice Nuclear Weapons School
ATTN: TTV 3416th TTSQ

Joint Chiefs of Staff
ATTN: J-3
ATTN: J-5 Nuclear Division
ATTN: SAGA

Joint Strat. Tgt. Planning Staff
ATTN: JL
ATTN: JP

Secretary of Defense Representative
Mutual & Balanced Force Reduction
ATTN: R. Clarke

National Defense University
ATTN: NWCLB-CR

U.S. Forces Korea
ATTN: CJ-P-G
ATTN: DJ-AM-SM

U.S. National Military Representative, SHAPE
ATTN: U.S. Documents Officer for Ops. (Nuc. Plans)

Undersecretary of Defense for Rsch. & Engrg.
ATTN: Strategic & Space Systems (OS)

## DEPARTMENT OF THE ARMY

Deputy Chief of Staff for Ops. & Plans
Department of the Army
ATTN: DAMO-NCC, V. Fenwick
ATTN: DAMO-SSW
ATTN: DAMO-RQS
ATTN: DAMO-SSP
ATTN: DAMO-ZD, C. Williams
ATTN: DAMO-NCN, J. Tengler

Deputy Chief of Staff for Rsch., Dev., & Acq.
Department of the Army
ATTN: DAMA-CSS-N, W. Murray
ATTN: DAMA-CSM-N
ATTN: Advisor for RDA Analysis, M. Gale

Deputy Undersecretary of the Army
ATTN: Operations Research, Mr. Lester

U.S. Army Air Defense School
ATTN: ATSA-CD-SC

DEPARTMENT OF THE ARMY (Continued)

Electronics Tech. & Devices Lab.
U.S. Army Electronics R&D Command
ATTN: DELEW, R. Freiberg

Harry Diamond Laboratories
Department of the Army
ATTN: DELHD-N-RBA, J. Rosado
ATTN: DELHD-N-TD, W. Carter
ATTN: DELHD-N-P, F. Balicki
ATTN: DELHD-N-CO, J. Ramsden

Measurement ECM & Support Technical Area
Department of the Army
ATTN: DRSEL-WL-M-M

Office of the Chief of Staff
Department of the Army
ATTN: DACS-DMO

Headquarters, 59th Ordnance Brigade
Department of the Army
ATTN: AEUSA-CDR

U.S. Army Armament Research & Dev. Command
ATTN: DRDAR-LCN-E

U.S. Army Ballistic Research Labs.
5 cy ATTN: DRDAR-BLV

U.S. Army Comb. Arms Combat Dev. Acty.
ATTN: ATCA-DLT
2 cy ATTN: ATCA-DLS

U.S. Army Concepts Analysis Agency
ATTN: D. Stevens
ATTN: C. Williams
ATTN: H. Hubbard

U.S. Army Elct. Warfare Lab.
ATTN: DELEW-M-FM, S. Megeath

U.S. Army Europe and Seventh Army
ATTN: AEAGC-O-N
ATTN: AEAGB
ATTN: AEAGD-MM

U.S. Army Forces Command
ATTN: AFOP-COE

U.S. Army Materiel Sys. Analysis Activity
ATTN: DRXSY-DS
ATTN: DRXSY-S

U.S. Army Materiel Dev. & Readiness Command
ATTN: DRCDE-DM

U.S. Army Missile Command
ATTN: DRSMI-YDR Foreign Intelligence Office

U.S. Army Nuclear & Chemical Agency
ATTN: Library for MONA-ZB
2 cy ATTN: Library for MONA-SAL

U.S. Army Ordnance & Chemical Center and School
ATTN: ATSL-CCC-M

U.S. Army TRADOC Systems Analysis Activity
ATTN: ATAA-TDC, J. Hesse

DEPARTMENT OF THE ARMY (Continued)

U.S. Army Training and Doctrine Command
ATTN: ATORI-IT-TA

U.S. Army War College
ATTN: AWCI, R. Rogan

V Corps
Department of the Army
ATTN: AETVFAS-F, P. Reavill

VII Corps
Department of the Army
ATTN: AETSFA-FSE
ATTN: AETSGB-O
ATTN: AETSGB-I
ATTN: AETSGC-O

DEPARTMENT OF THE NAVY

David Taylor Naval Ship R&D Center
ATTN: Code 174/Code 186

Naval Academy
ATTN: Nimitz Library/Technical Rpts. Branch

Naval Material Command
ATTN: MAT-OON

Naval Ocean Systems Center
ATTN: Research Library

Naval Postgraduate School
ATTN: Code 1424

Naval Research Laboratory
ATTN: Code 6600
ATTN: Code 7944
ATTN: Code 1409
ATTN: Code 4100
ATTN: Code 1400
ATTN: Code 6110
ATTN: Code 6100

Naval Surface Weapons Center
ATTN: Code F31
ATTN: Code F32, W. Emberson
ATTN: Code X211

Naval War College
ATTN: 12
ATTN: Center for War Gaming

Naval Weapons Center
ATTN: Code 31707

Naval Weapons Evaluation Facility
ATTN: Code AT

Nuclear Weapons Tng. Group, Atlantic
Department of the Navy
ATTN: Technical Library

Office of Naval Research
ATTN: Code 713

Office of the Chief of Naval Operations
ATTN: OP 604C

## DEPARTMENT OF THE NAVY (Continued)

Plans Division
Plans & Policies Department
Headquarters Marine Corps (Code PL)
ATTN: Joint Strategic Branch

Commander-in-Chief
U.S. Atlantic Fleet
Department of the Navy
ATTN: Code J-34
ATTN: Code J-54

Commander-in-Chief
U.S. Naval Forces, Europe
ATTN: N326, R. Thomas

## DEPARTMENT OF THE AIR FORCE

Aeronautical Systems Division
Air Froce Systems Command
ATTN: XRO/MAR, J. Sherrod

Aerospace Defense Command
ATTN: ADCOM/INA

Air Force Armament Laboratory
ATTN: AFATL/DLY

Air Force Weapons Laboratory
Air Force Systems Command
ATTN: NSSB
ATTN: AFWL SA
ATTN: NTN
ATTN: SUL

Assistant Chief of Staff
Studies & Analyses
Department of the Air Force
ATTN: AF/SAMI

Deputy Chief of Staff
Operations, Plans and Readiness
Department of the Air Force
ATTN: AFXOXF, R. Linhard
ATTN: AFXOXFM

Deputy Chief of Staff
Research, Development, & Acq.
Department of the Air Force
ATTN: AFRDQSM

Strategic Air Command
Department of the Air Force
ATTN: NRI

Tactical Air Command
Department of the Air Force
ATTN: XPSC
ATTN: XPS
ATTN: DRA

Commander-in-Chief
U.S. Air Forces in Europe
ATTN: XPX
ATTN: XPXX
ATTN: INAT

## DEPARTMENT OF ENERGY

Department of Energy
ATTN: Document Control for OMA, D. Hoover

## DEPARTMENT OF ENERGY (Continued)

Department of Energy
ATTN: DOE/ISA

## DEPARTMENT OF ENERGY CONTRACTORS

Lawrence Livermore Laboratory
ATTN: Document Control for L-9, R. Barker
ATTN: Document Control for L-9, D. Blumenthal
ATTN: Document Control for L-21, M. Gustavson

Los Alamos Scientific Laboratory
ATTN: Document Control for G. Best

Sandia Laboratories
ATTN: Document Control for 1313, T. Edrington
ATTN: Document Control for Sys. Studies Div. 1313
ATTN: Document Control for J. Kaizur

## DEPARTMENT OF DEFENSE CONTRACTORS

Advanced Research & Applications Corp.
ATTN: R. Armistead

AVCO Research & Systems Group
ATTN: J. Gilmore
ATTN: G. Grant

Battelle Memorial Institute
ATTN: D. Hamman

BDM Corp.
ATTN: J. Braddock

BDM Corp.
ATTN: T. McWilliams

66th MI Group
ATTN: RDA, T. Greene
ATTN: F. Payne

General Electric Company—TEMPO
ATTN: DASIAC

General Research Corp.
ATTN: P. Lowry
ATTN: H. Schroeder

Horizons Technology, Inc.
ATTN: R. Kruger

Hudson Institute, Inc.
ATTN: H. Kahn

Hughes Aircraft Co.
ATTN: H. Ward

JAYCOR
ATTN: S. Brucker

JAYCOR
ATTN: R. Sullivan
ATTN: E. Almquist

Kaman Sciences Corp.
ATTN: F. Shelton

LFE Corp.
ATTN: M. Nathans

DEPARTMENT OF DEFENSE CONTRACTORS (Continued)

Lockheed-California Co.
ATTN: G. Busch

Mathematical Applications Group, Inc.
ATTN: M. Cohen

McMillan Science Associates, Inc.
ATTN: W. McMillan

Mission Research Corp.
ATTN: D. Sowle

Pacific-Sierra Research Corp.
ATTN: G. Lang

R & D Associates
ATTN: S. Cohen
ATTN: A. Latter
ATTN: C. MacDonald

R & D Associates
ATTN: R. Latter

Rand Corp.
ATTN: W. Jones
ATTN: Library

Santa Fe Corp
ATTN: D. Paolucci

Science Applications, Inc.
ATTN: W. Layson

DEPARTMENT OF DEFENSE CONTRACTORS (Continued)

Science Applications, Inc.
ATTN: J. Martin
ATTN: M. Drake

SRI International
ATTN: P. Dolan
ATTN: D. Elliott
ATTN: R. Monahan
ATTN: E. DuBois

SRI International
ATTN: W. Berning
ATTN: R. Foster

Systems, Science & Software, Inc.
ATTN: K. Pyatt

Systems, Science & Software, Inc.
ATTN: J. Cane

Technology Service corp.
ATTN: S. Canby

Tetra Tech, Inc.
ATTN: F. Bothwell

TRW Defense & Space Systems Group
ATTN: P. Dai

Vector Research, Inc.
ATTN: S. Bonder